DEFENCE S&T TECHNICAL BULLETIN

VOL. 8 NUM. 1 YEAR 2015 ISSN 1985-6571

CONTENTS

STRIDE

SCIENCE & TECHNOLOGY RESEARCH INSTITUTE FOR DEFENCE

AIMS AND SCOPE

The Defence S&T Technical Bulletin is the official technical bulletin of the Science & Technology Research Institute for Defence (STRIDE). The bulletin, which is indexed in, among others, Scopus, Index Corpenicus, ProQuest and EBSCO, contains manuscripts 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 manuscript is accepted on the understanding that it is an original piece of work which has not been accepted for publication elsewhere.

PRESENTATION OF MANUSCRIPTS

The format of the manuscript is as follows:

a) Page size A4
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. Dinesh Sathyamoorthy (dinesh.sathyamoorthy@stride.gov.my)
2) Dr. Mahdi bin Che Isa (mahdi.cheisa@stride.gov.my)

The next edition of the bulletin (vol. 8, num 2) is expected to be published in November 2015. The due date for submissions is 2 September 2015. **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.

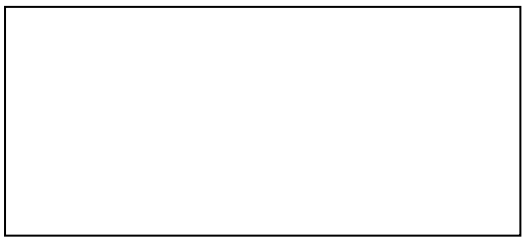


Figure 1: Title of figure.

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:

Books

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

Book Chapters

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

Journals / Serials

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

Online Sources

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).

Unpublished Materials (e.g. theses, reports and documents)

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

EVALUATION OF THE SUITABILITY OF FLY ASH POWDER FOR ATMOSPHERIC PLASMA SPRAY

Mohd Moesli Muhammad[1], Azman Jalar[2], Roslinda Shamsudin[2*] & Mahdi Che Isa[1]

[1]Maritime Technology Division (BTM), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[2]School of Applied Physics, Faculty of Science and Technology, Universiti Kebangsaan Malaysia (UKM), Malaysia

[*]Email: linda@ukm.edu.my

ABSTRACT

This study describes the potential of sieved fly ash powders to be used as feed stock materials in atmospheric plasma spray. The analyses that were carried out were particle size distribution (PSD), chemical composition, morphology and flowability. The PSD analysis showed that most of the fly ash powders were fine particles of less than 63 μm. The chemical analysis showed that the main components of the fly ash powders were iron, silica, calcium, aluminium and potassium. The morphological analysis showed that the coarse and medium sized fly ash particles consist of irregular and spherical shapes, whereas the fine particles were dominated by spherical shapes. The flowability study showed that the medium sized particles (63–100 μm) are suitable to be used as plasma spray powders due to free flowing and no blockages within the powder injector during the spraying process. On the other hand, the fine particles failed to be delivered within the plasma spray pipeline system due to powder agglomeration.

Keyword: *Fly ash; atmospheric plasma spray*; *particle size distribution (PSD); flowability; powder agglomeration.*

1. INTRODUCTION

Fly ash is an industrial by-product that is generated in huge quantities during the combustion of coal for energy production. It is generally grey in colour, abrasive, mostly alkaline and refractory in nature. Chemical analysis has shown that silicon oxide (SiO_2), aluminium oxide (Al_2O_3), iron oxide (Fe_2O_3) and titanium oxide (TiO_2) are its major constituents (Ahmaruzzaman, 2010; Valentim *et al*., 2012). Metal oxides in fly ash have advantages in terms of high hardness, good wear and corrosion resistance, which are desirable properties for protective coatings (Yu *et al*., 2012; Tiwari *et al*., 2014). Due to the high demand for electricity and cost competitiveness of coal-based power plants for power production, it is expected that the generation of waste from coal, such as fly ash, will increase in the future. A number of attempts have been made to use this waste material for plasma spray coatings (Krishna *et al*., 2003; Okumus *et al*., 2004). Atmospheric plasma spray is an expensive technique due to the high cost of the manufacturing process for spray grade powders. As fly ash is cheaper and readily available as industrial waste, it can be used as a cheaper alternative for spray grade powders.

Due to their potential to be used as feed stock materials in plasma spray, information on particle size distribution (PSD) is essential. PSD analysis is performed to determine the particle sizes and range of representative powders (Bentz *et al*., 2011; Linak *et al*., 2002). Many methods are available to evaluate PSD, such as sieving, and image and laser diffraction analyses (Joanne, 1998; Stefano *et al*., 2010; Tobias &Thurley, 2011). Sieving is a well known method that is able to separate particles into different groups. This method has been used in the powder manufacturing industry to classify particles into specific ranges

of groups. Therefore, it is the most suitable method for fly ash powders due to the wide range of particle sizes that are not desirable for plasma spray application (Padmanabhan *et al*., 2007; Demnati *et al*., 2014).

The objective of this work is to evaluate the properties of fly ash powders obtained from a local thermal power plant and their suitability as feed stock material for atmospheric plasma spray. The analyses carried out are PSD, chemical composition, morphology and flowability.

2. MATERIALS AND METHODS

The as-received fly ash sample used in this study was collected from a Tenaga Nasional Berhad (TNB) coal-fired power plant located at Seri Manjung, Perak, Malaysia. The measurement of PSD was carried out using a mechanical sieve shaker (model Retsch). The collected sample was screened through a set of seven different sieves, with opening sizes of 38, 45, 63, 75, 100, 125 and 250 μm. The sieved fly ash powders produced eight classified fractions (Table 1). The duration of the sieve process was set at 30 min with the shaker acceleration set at amplitude of 1.00 mm/g. The distributions of the fractions were determined by the difference between the initial and final weights of each sieve.

Table 1: Classification of fractions of the sieved fly ash powders.

Fraction	Retained by (μm)	Particle range (μm)
A	250	Above 250
B	125	+125 to -250
C	100	+100 to -125
D	75	+75 to -100
E	63	+63 to -75
F	45	+45 to -63
G	38	+38 to -45
H	Collecting pan	Below 38

The chemical composition analysis was conducted using a wavelength dispersive X-ray fluorescence (WDXRF) spectrometer (Bruker SP 4 Pioneer) equipped with an Rh X-ray tube and 4 kW generator. The results were presented in weight percentages (wt%). For the sieved samples, the bulk densities of the different groups of the fly ash were determined by weighing the powders which were filled in a cup with volume of 25 cm^3. The morphologies of the three groups of particles (coarse, medium sized and fine) were observed using a scanning electron microscope (SEM)(Zeiss 1430VP) with a X-ray (EDS) spectrometer analyser.

The flowability of the fly ash powders was evaluated using the powder feeder of a Praxair plasma spray system. The test was performed on the sieved powders at carrier gas pressure of 45 psi and powder feed rate of 3 rpm. These values were selected based on the maximum operating level of the plasma spray system for both parameters. The evaluation of the powders' flowability was based on visual observation of the powder injector after the spraying process, in which the powders flow through the pipeline from the powder feeder (Figure 1).

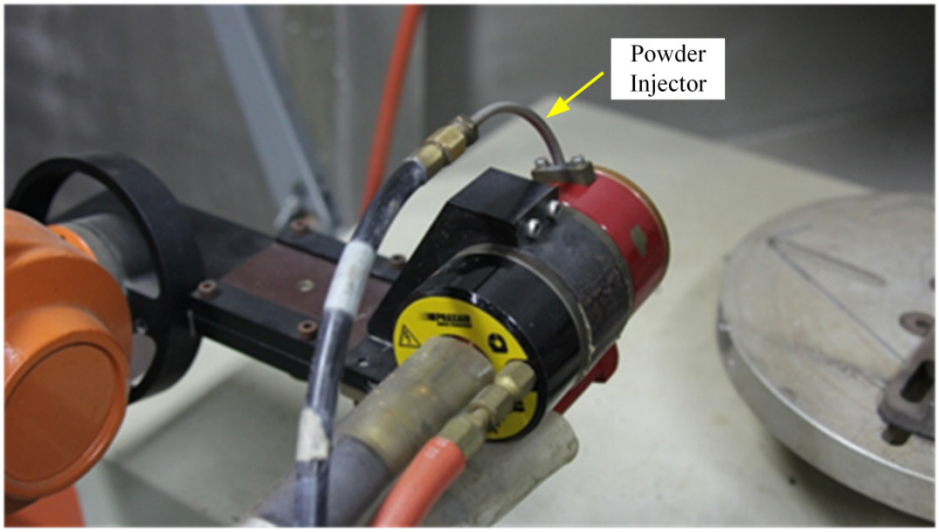


Figure 1: The powder injector in the plasma spray system.

3. RESULTS AND DISCUSSION

3.1 Particle Size Distribution (PSD)

Figure 2 shows the histogram of the PSD of the fly ash powders. The graph shows that the PSD is dominated by the F, G and H fractions, which are particles below 63 μm. This is followed by the D and E fractions, which are particles in the range of +63 to -100 μm, while the remaining fractions, A, B and C, have particles size of above 100 μm. Most of the fly ash particles are fine powders. Due to the significant difference between the left (coarse) and right (fine) sides of the PSD, the sieved fly ash powders are divided into three groups, which are coarse, medium sized and fine particles. The coarse particles, with size of more than 100 μm (fractions A, B and C) represent only 4wt%, while the medium sized particles, in the range between 63 and 100 μm (fractions D and E) has 24wt%. Fine sized particles (below 63 μm) dominated the analysed fly ash sample with 72wt% (fractions F,G and H), as shown in Figure 3. According to Sarkar *et al*. (2006), the high percentage of fine particles in the fly ash shows the efficiency of coal combustion due to complete burning of feed coal.

3.2 Chemical Composition and Morphology

The chemical composition of the fly ash powders is shown in Table 2. The main major elements were iron, silicon, calcium, aluminium, potassium, titanium and magnesium, which range between 1 to 32 wt%. Other elements having less than 1 wt% were strontium, sulphur, phosphorous, barium, manganese, zinc and nickel while chromium, copper, rubidium and zirconium were detected as trace elements with range between 0.01 to 0.06 wt%. According to ASTM (2003), the classification of fly ash is based on the composition of calcium (Ca), and the total composition of three elements, silicon (Si), iron (Fe) and Aluminium (Al). The fly ash can be classified into two categories, which are Classes F and C. For the Class F fly ash, the total composition of the three elements (Si, Fe and Al) is more than 70% and the Ca composition is lower than 20%. On the other hand, for the Class C fly ash, the total composition of Si, Fe and Al is in the range of 50 to 70% and calcium composition is more than 20%. In this study, the fly ash used has a total composition of 68% (Fe, Si and Al) and 22% calcium, and hence, is classified as Class C fly ash.

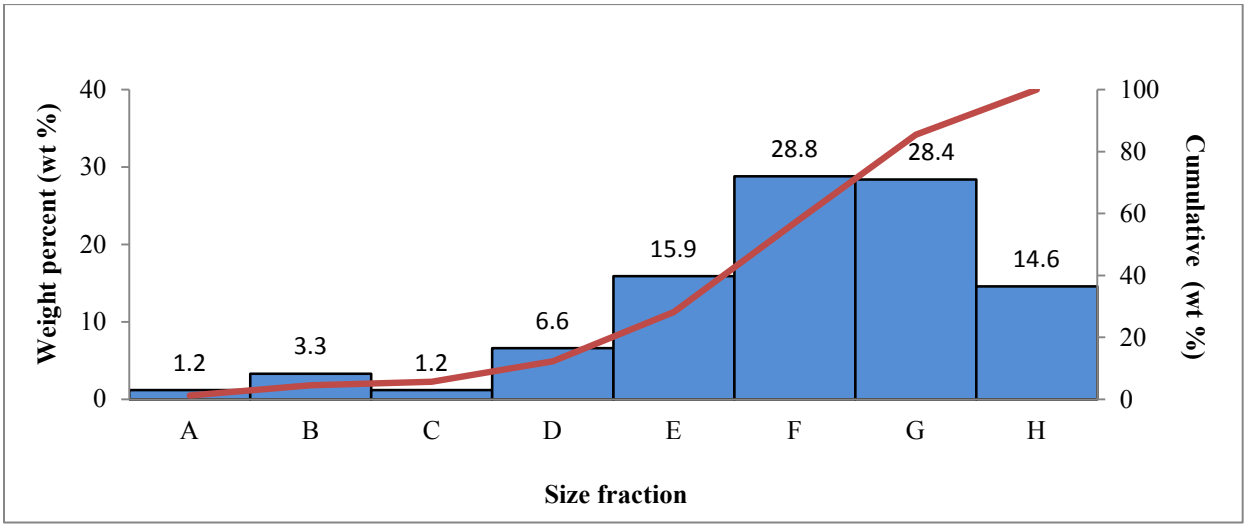


Figure 2: Histogram of the PSD of the fly ash powders using the sieve method.

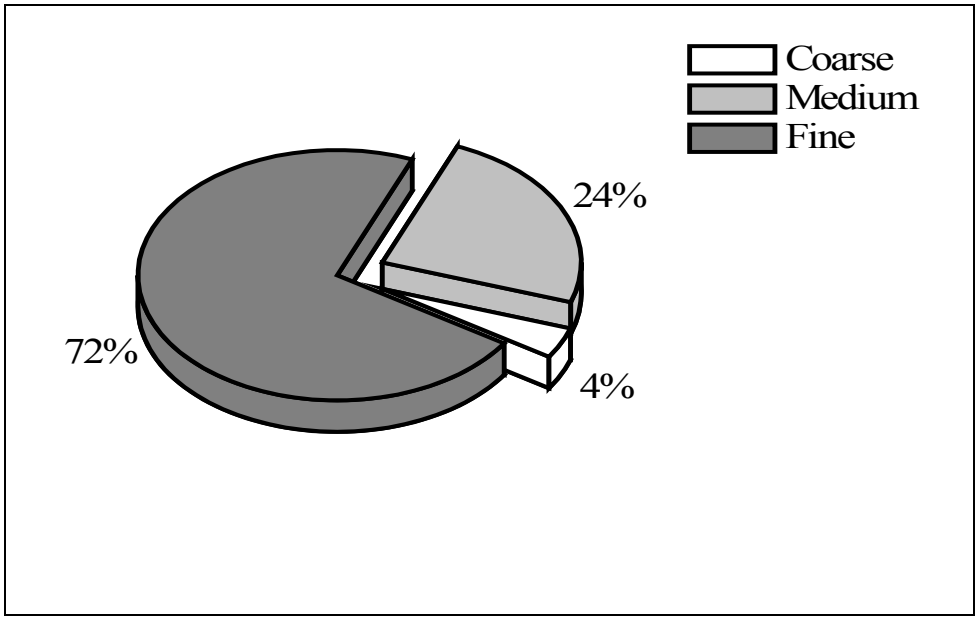


Figure 3: Particle distribution based on the three classified sizes; coarse, medium and fine.

Table 2: Chemical composition of the as-received fly ash powders.

Elements	Content (wt%)
Iron (Fe)	32.62
Silicon (Si)	24.18
Calcium (Ca)	22.17
Aluminium (Al)	10.74
Kalium (K)	4.04
Titanium (Ti)	1.72
Magnesium (Mg)	1.22
Strontium (Sr)	0.49
Sulphur (S)	0.83
Phosphorous (P)	0.79
Barium (Ba)	0.50
Manganese (Mn)	0.33
Zinc (Zn)	0.11
Nickel (Ni)	0.11
Cromium (Cr)	Trace
Copper (Cu)	Trace
Rubidium (Rb)	Trace
Zirconium (Zr)	Trace

Figure 4 shows the SEM micrographs of the three types of fly ash groups. Most of the particles that belong to the coarse fly ash have irregular shapes (Figure 4(a)). The elemental analysis indicated that the coarse particles (P1 and P2) are rich in iron-silica, whereas the unburned coal based on high peak of carbon is detected and represented by P3. The medium sized particles have spherical and irregular shapes (Figure 4(b)), with the fraction of the spherical shapes higher than the irregular shapes. Most of the particles (P4, P5 and P6) detected are rich in Al, Fe and Si elements. The fine particles of the fly ash (Figure 4(c)) have solid spherical shapes and their chemical composition is similar to the medium sized particles.

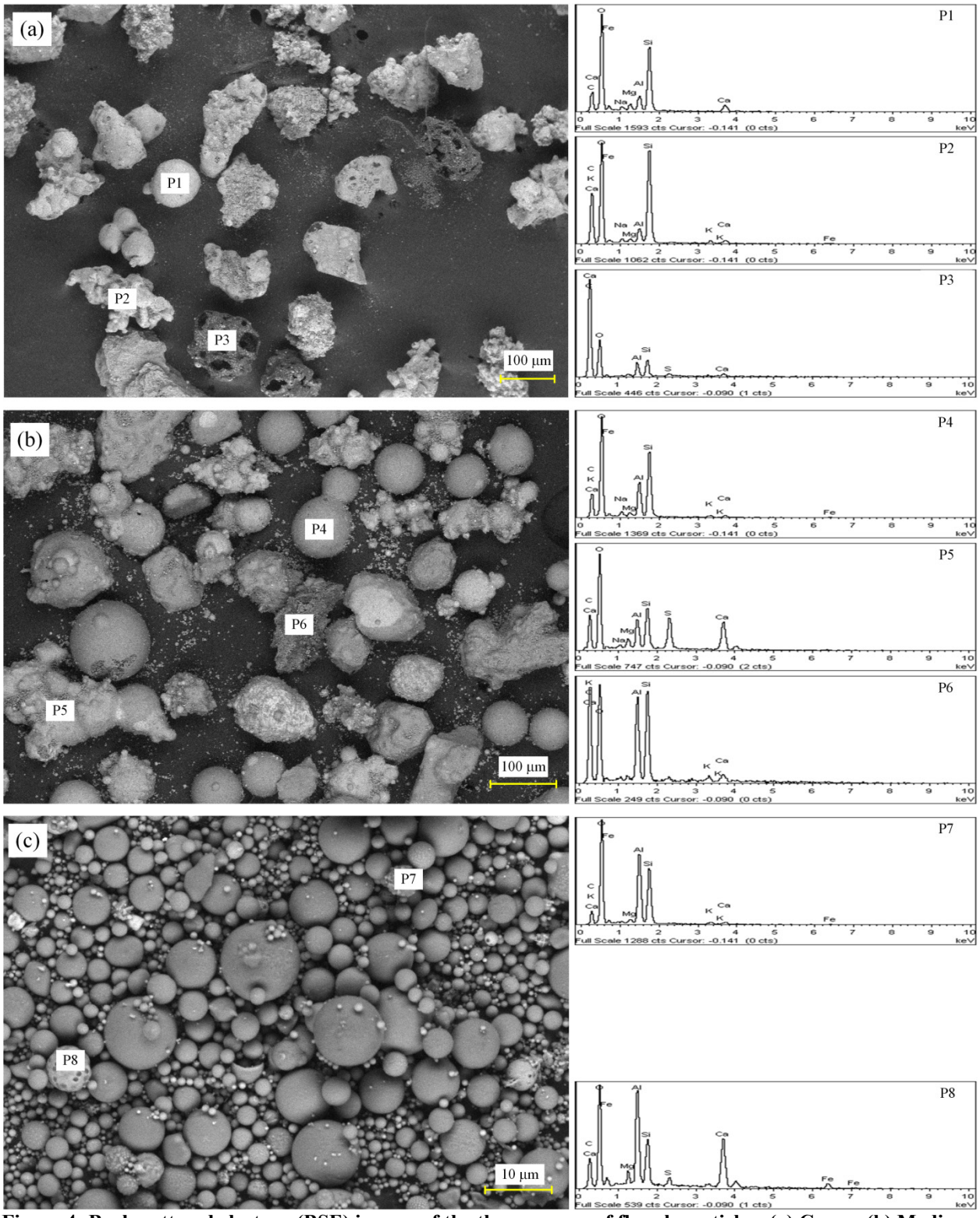


Figure 4: Backscattered electron (BSE) images of the three groups of fly ash particles: (a) Coarse (b) Medium (c) Fine.

3.3 Flowability

A simple test of powder flowability was carried out on the powder feeder of a Praxair plasma spray system. Only medium sized and fine particles were selected because the coarse particles contain a lot of unburned carbon, which is not suitable for plasma spraying. After the spraying process, visual observation was carried out on the pipeline to observe any blockages in the pipeline system. The fine particles, dominated by spherical shapes, blocked the powder injector pipeline because of poor feeding, with agglomeration occurring when the powders travelled through pipeline tube from the feeder to the powder injector (Figure 5(a)). The agglomeration process occurred due to adhesive forces that exist among the small particles which attract each other to form larger particles. For the medium sized particles (Figures 5(b)), visual examination shows a stable condition with no agglomeration effect and remain as individual particles.. The differences in morphologies of the sieved fly ash particles are due to coal combustion temperature and post-combustion in the boiler (Kutchko & Kim, 2006). In this analysis, it was found that the medium sized particles have good flowability characteristic as no deposited particles were found in the system and thus, have great potential to be used as plasma spray powders.

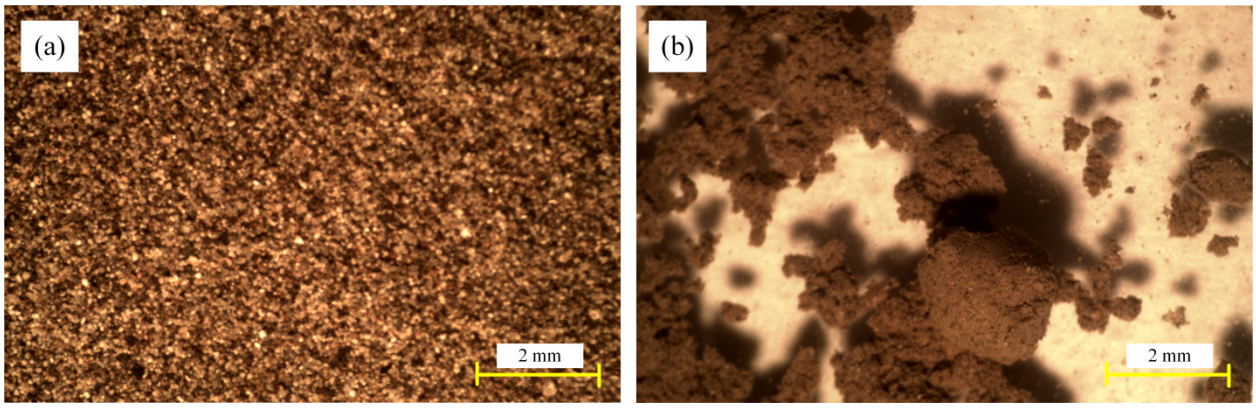


Figure 5: Optical observation of the physical appearances of the two groups of fly ash particles used for the flowability test: (a) Medium (b) Fine.

4. CONCLUSION

In this study, PSD, chemical composition, morphology and flowability analyses were carried out on the fly ash powders to determine their suitability as feed stock materials in atmospheric plasma spray. The PSD analysis indicated that most of the fly ash powders are fine particles. The chemical composition analysis showed that the main elements in the fly ash powders are iron, silica, calcium, aluminium and potassium (more 4 than wt%). From the morphology analysis, it was observed that most of the spherical shaped fly ash particles were found in the fine particles, mixed with irregular shapes in the medium sized particles, and of lower quantity in the coarse particles. The flowability analysis demonstrated that the medium sized particles, in the range of 63 to 100 μm, are suitable to be used as plasma spray feedstock, while the fine particles failed to travel within plasma spray pipeline system due powder agglomeration.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the Ministry of Education and Universiti Kebangsaan Malaysia (UKM) for providing research funds DPP-2013-035and FRGS-2-2013-SG06-UKM-02-6. The first author thanks the Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence for awarding study leave to him.

REFERENCE

Ahmaruzzaman M. (2010). A review on the utilization of fly ash. *Prog Energy Combust*. Sci. **36**: 327–363.

ASTM (2003). *ASTM C 618-03: Standard Specification for Coal Fly Ash and Raw or Calcined Natural Pozzolan for Use in Concrete*. ASTM international, USA.

Bentz, D., Hansen, A.S. & Guynn, J.M. (2011). Optimization of cement and fly ash particle sizes to produce sustainable concretes. *Cem. Concr. Compos*. **33**: 824-831.

Demnati, I., Grossin, D., Errassifi, F., Combes, C., Rey, C. & Bolay, N. (2014). Synthesis of fluor-hydroxyapatite powder for plasma sprayed biomedical coatings: Characterization and improvement of the powder properties. *Powder Technol*. **255**: 23-28.

Joanne, M.R. (1998). The effect of particle form on sieve analysis: a test by image analysis. *Eng. Geol.* **50**:111-124.

Krishna, L., Sen, D. & Rao, D. (2003). Coatability and characterization of fly ash deposited on mild steel by detonation spraying. *J. Therm. Spray Technol*. **12**: 77-79.

Kutchko, B.G. & Kim, A.G. (2006). Fly ash characterization by SEM-EDS. *Fuel*, 85: 2537–2544.

Linak, W.P., Miller, A., Seames, W.S., Wendt, J.O., Ishinomori, T., Endo, Y. & Miyamae, S. (2002). Ontrimodal particle size distribution in fly ash from pulverized coal combustion. *Proc. Comb Inst*. **29**:441-447.

Okumus, S.C., Demirkyran, A.S. & Bindal, C.(2004). Fly ash bases plasma spray coating. *Key Eng. Mater.* **264–268**: 533–536.

Padmanabhan, P.V.A., Ramanathan, S., Sreekumar, K.P., Satpute, R.U. Kutty, T.R.G., Gonal, M.R. & Gantayet, L.M. (2007). Synthesis of thermal spray grade yttrium oxide powder and its application for plasma spray deposition. *Mater. Chem. Phys*. **106**: 416-421.

Tiwari, M., Sahu, S., Bhangare, R.C., Ajmal, P.Y. & Paudit, G.G, (2014). Elemental characterization of coal, fly ash and bottom ash using an energy dispersive X-ray fluorescence technique. *Appl. Radiat. Isot.* **90**: 53-57.

Tobias, A. & Thurley, M.J. (2011). Minimizing profile error when estimating the sieve-size distribution of iron ore pellets using ordinal logistic regression. *Powder Technol*. **206**: 218-226.

Sarkar, A., Rano, R., Udaybhanu, G. & Basu, A.K. (2006). A Comprehensive characterisation of fly ash from a thermal power plant in eastern India. *Fuel Process. Technol*. **87**: 259-277.

Stefano C.D., Ferro, V. & Mirabile, S. (2010). Comparison between grain-size analyses using laser diffraction and sedimentation methods. *Biosyst. Eng*. **106**: 205-215.

Valentim, B., Guedes, A., Flores, D., Ward, C.R. & Hower, J.C. (2009). Coal combustion and gasification products. *Coal Combust. Gasif. Prod*. **1**: 14-24.

Yu, J., Li, X., Fleming, D., Meng, Z., Wang, D. & Tahmasebi, A. (2012). Analysis on characteristics of fly ash from coal fired power stations. *Energy Procedia* **17**: 3-9.

ELECTROCHEMICAL IMPRINTED SOL-GEL FILMS FOR DETECTION OF ORGANOPHOSPHATE CHEMICAL WARFARE AGENT

Wan Norfazilah Wan Ismail[1*] & Atsunori Matsuda[2]

[1]Protection & Biophysical Technology Division (BTPB), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[2]Department of Electrical and Electronic Information Engineering, Toyohashi University of Technology (TUT), Japan

[*]Email: norfazilah.ismail@stride.gov.my

ABSTRACT

The present study was undertaken to detect organophosphate chemical warfare agents via electrochemistry by utilising a molecular imprinted (MIP) sol-gel hybrid 3-cyanopropyltriethoxysilane (CNPrTEOS) film on indium tin oxide (ITO) glass substrate. The MIP film was formed by dip-coating on the ITO glass substrate through strong Si-O-Si bonds for selective, rapid and ultra-trace detection of organophosphate chemical warfare agent in a cyclic voltammetry (CV) device. The surface morphology and coating thickness of the MIP sol-gel hybrid CNPrTEOS film was characterised by using field emission scanning electron microscope. The blocking/insulating property of the MIP sol-gel hybrid film was studied using ferricyanide ions redox couple measurement. The CV peak current in the presence of different concentrations of the selected analyte showed a good linear correlation (R^2 = 0.9977) in the range 0.5 to 10 pg mL^{-1} with a limit of detection (signal to noise ratio = 3) of 0.2446 pg mL^{-1}.

Keywords: *Sol-gel hybrid; molecular imprinted (MIP) film; electrochemical sensor; cyclic voltammetry (CV); organophosphate chemical warfare agent.*

1. Introduction

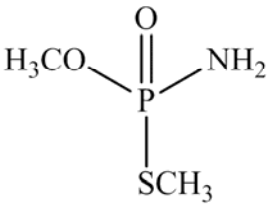
A number of organophosphate insecticides such as methamidophos, malathion and parathion are nerve agents acting on the enzyme acetylcholinesterase (AChE). Irreversible inhibition of AChE can result in possible death of humans (Newmark, 2004). Organophosphate insecticides are considered to be chemical warfare agents or chemical weapons if they are produced and stockpiled in amounts that exceed the requirements for purposes that are not prohibited under the Chemical Weapons Convention (CWC). There is an incidence of nerve agents being used as chemical weapons in human history and many countries. They were used against the Kurds in Iraq (Black *et al*., 1994) and also in the terrorist attack on the Tokyo subway in 1995 (Nozaki & Aikawa, 1995). Research into new chemical weapons, their production and use still continue in different areas around the world (Bismuth *et al*., 2004).

The determination and quantification of chemical warfare agent in a precise, convenient and economical fashion is an important goal that has been achieved only partially as these chemicals can be difficult to detect by conventional means (Noort *et al*., 2002; Sadik *et al*., 2003; Fitch *et al*., 2003; Stewart & Sullivan Jr., 1992). In many cases, when chemical warfare agents or chemical weapons are present as contaminants, the first handling step is extraction followed by separation of the matrices before attempting to identify the types of chemicals present in the sample via a detector. Separation techniques such as liquid chromatography (LC), (Wada *et al*., 2006) gas chromatography (GC) (Haas, 1998) and capillary electrophoresis (Nassar *et al*., 1999) have proven successful methods for chemical warfare agent sample separation. These separation techniques are usually coupled to mass spectroscopy (MS) as a detection method (Kimm *et al*., 2002; Wada *et al*., 2006). Due to their physical properties, the method of choice for chemical warfare agents' analytical handling is GC-MS (Diaz *et al*., 2004), where it is the only approved technology for nerve agent identification by the Organization for the Prohibition of Chemical Weapons (OPCW). Although GC-MS has some

advantages over LC-MS, such as its simple mobile phase which avoids issues such as reagent incompatibility, pH and solvent mix (Guodong & Lin, 2006), LC-MS is a good alternative for analysis of chemical weapon aqueous samples. Unfortunately, these laboratory techniques require large pieces of equipment, controlled conditions and highly trained personnel to conduct such experiments.

Electrochemical detectors have the potential to overcome the shortcomings associated with the present detection technologies. In electrochemical sensors, a working electrode is used to measure the electrochemical response of the system in the form of either potential or current signal. Measurements are often carried out in solution in the presence of an analyte by using the electrochemical properties of the nerve agent or of a chemical reaction that can be detected electrochemically (Wang *et al.*, 2008). Electrochemical detectors are potentially sensitive and selective and can be used for continuous monitoring. They also exhibit a wide linear response, minimal space and power requirements and are cost efficient.

In the present study, a cyano-based sol-gel hybrid film was constructed and molecularly imprinted (MIP) with selected organophosphate chemical warfare agent namely, methamidophos, for sensing applications. The novel cyano-based MIP sol-gel hybrid film was coated on indium tin oxide (ITO) glass substrate as a working electrode in cyclic voltammetry (CV) test for the detection of polar methamidophos with log $K_{o/w}$ = -1.74. The MIP and reference non-imprinted polymer (NIP) sol-gel hybrid film-coated ITO glass were used as the working electrodes to record the oxidation peak currents by CV in the phosphate buffer solutions (PBS) containing methamidophos (Scheme 1). The detector has been tested with respect to sensitivity, linearity and detection limit.



Scheme 1: Chemical structure of methamidophos.

2. MATERIALS AND METHODS

2.1 Reagents

3-cyanopropyltriethoxysilane (98%, CNPrTEOS) was purchased from Sigma Aldrich (St. Louis, MO, USA) and tetraethoxysilane (95%, TEOS) from Wako Pure Chemical Ind., Ltd. (Osaka, Japan). Hydrochloric acid (HCl) and deionised water were used for hydrolysis of functional monomers in polymerization process. The deionised water was obtained from a Millipore 106 Simplicity 185 (UV) water system from Thermo Scientific (Barnstead, MA, USA). Potassium ferricyanide ($K_3Fe(CN)_6$) was purchased from Wako Pure Chemical Ind., Ltd. (Osaka, Japan). Methamidophos (98.5%) was purchased from Sigma Aldrich (St. Louis, MO, USA). The standard stock solution was prepared by dissolving the standard pesticides in ethanol and kept at 4°C until used. They were diluted to required concentration using 0.05 M phosphate buffer solution (PBS). 0.1M potassium chloride (KCl) was used as a supporting electrolyte. All analyte solutions were prepared daily in 0.05M PBS (pH 7.0) and purged with nitrogen for 10 min prior to use. Other reagents were commercially available as analytical grade reagents and used without further purification.

2.2 Equipment

Cyclic voltammetry measurements were performed using an electrochemical analyser model HSV-100 (Hokuto Denko Co. Ltd., Tokyo, Japan) connected to a personal computer. A homemade electrochemical cell (5 mL), fitted with a gas bubbler and a three-electrode configuration consisting of indium tin oxide (ITO)-coated glass substrates (20 mm × 5 mm × 1.1 mm, 10 Ω/sq, Avan Strate Inc.) as working electrodes, a platinum wire, 2 cm long with a diameter of 0.3 mm as counter electrode and Ag/AgCl (saturated KCl) as a reference electrode. A field emission scanning electron microscope (FE SEM, Hitachi S-4800, Hitachi High-Tech., Tokyo, Japan) was used to characterize the surface morphology and thickness of the film.

2.3 Electrode Preparation and Procedures

2.3.1 Imprinted Sol-Gel Film Preparation

The sol-gel hybrid CNPrTEOS film was synthesised by drop wise addition of 0.67 mL of tetraethoxysilane (TEOS, 30% v/v) into 5 mL sample bottle containing 1 mL 0.10 M hydrochloric acid (HCl) as catalyst in 2.16 mL water. 2.4 mL cyanopropyltriethoxysilane (CNPrTEOS) was added dropwise into the same volume of HCl and water. Each solution was stirred for 45 min, and then the TEOS solution was poured into the CNPrTEOS solution. The mixture was further stirred at 450 rpm for 30 min. The homogenous CNPrTEOS sol was aged at room temperature before used in molecularly imprinting process. All procedures were conducted at room temperature. The MIP was prepared by thoroughly mixing a 4.5 mL of sol-gel hybrid CNPrTEOS sol obtained with 0.5 mL of 10 pg mL^{-1} ethanolic methamidophos for 15 min. The remaining sol-gel hybrid CNPrTEOS sol was used for the reference non-imprinted film (NIP), with the same procedure was applied.

2.3.2 Pretreatment and Modification of ITO-Coated Glass Substrate

Before coating with the MIP and NIP sol-gel hybrid film, the ITO glass substrate was cleaned with RCA solution (Kern & Puotinen, 1970), rinsed with deionized water and dried using nitrogen gas blowing. The ITO glass substrate was covered with a strip of clear tape to achieve an uncovered electrode surface area of 50 mm^2 before dip-coating with the MIP or NIP sol-gel hybrid CNPrTEOS sol. The dip coating process was performed using a dip coater (DC4200, Aiden Co. Ltd., Shinshiro, Japan) at a constant rate of 0.1 mm s^{-1}. After the dip-coating process, the clear tape was removed. The MIP sol-gel hybrid CNPrTEOS-coated ITO glass was air-dried for 30 min before rinsed with the PBS to remove any physically adsorbed materials.

Methamidophos was removed from the imprinted film using ultrasonic desorption in ethanol for 2 min. Then the electrode was rinsed with deionized water and dried under nitrogen flow before use. Reference NIP film was rinsed with ethanol to remove any unreacted materials.

2.3.3 Electrochemical Measurements

The sol-gel film-coated ITO glass was dipped in 3 mL of appropriate concentrations of methamidophos in PBS (pH 7.0) for 7 min with stirring (150 rpm) at room temperature for pre-concentration effect. Then, the sol-gel hybrid film-coated ITO glass was washed with distilled water to remove any physically absorbed compounds on the electrode surface, before transferred into the electrochemical cell. The electrolyte solution was purged with nitrogen for 10 min before electrochemical measurements. CV measurements of methamidophos were recorded in 0.05 M PBS (pH 7.0) and 0.1 M KCl in the potential range of -1.0 to +1.2 V vs. Ag/AgCl at a scan rate of 100 mV s^{-1}. The blocking/insulating properties of the MIP sol-gel hybrid film was studied in the presence of $[Fe(CN)_6]^{3-}/[Fe(CN)_6]^{4-}$ redox couple measurements in the potential range of -0.2 V to +0.6 V at a scan rate of 100 mV s^{-1}. All measurements were performed at room temperature in triplicates.

3. RESULTS AND DISCUSSION

3.1 Preparation of the Modified Electrode

Glass substrate coated with ITO film is able to conduct electricity, thus it is very useful in CV measurement. In addition, pretreatment of ITO-coated glass substrate by Radio Corporation of America (RCA) method (Kern & Puotinen, 1970) has activated the ITO surface and allowed the MIP sol-gel hybrid film to covalently bind to the ITO film on the glass substrate (Gao *et al*., 2007). Such bonding will enhance the lifetime of the modified working electrode as compared to physically coated film onto commonly used electrode such as glassy carbon electrode (Xie *et al*., 2010; Li *et al*., 2005).

The use of MIP technique in electrochemical sensing field has become a very important tool to develop suitable recognition elements with specific recognition sites (Atta & Abdel-Mageed, 2009; Yang *et al*., 2009; Li *et al*., 2012). Some of them are cavities with sizes matching the template molecule. These are template recognition sites, constructed with regular and perfect shape in the polymerization period and thus have good affinity for the template molecule (Li *et al*., 2012). The other reason for the observed high selectivity of the template molecules is the presence of functional monomers in the polymer matrix which form specific binding cavities by leaving the template molecule from the polymers. The specific binding cavities matched with the template molecules, similar to the active sites in an enzyme (Hu *et al*., 2012).

The use of hybrid film is a very significant factor in material design. CNPrTEOS possesses hydroxyl and cyano-group that can form hydrogen bond with amino-group in methamidophos and also allow polar interaction with polar methoxy and methylthio group in methamidophos. The propyl group in CNPrTEOS introduces additional hydrophobicity to the resultant materials. It is known that the hybrid film is able to promote the rebinding ability of template molecules to the imprinted film (Shustak *et al*., 2003; Marx *et al*., 2004; Pater *et al*., 2009). On the contrary, there are no imprinted cavities in the reference NIP sol-gel hybrid film that could be opened, thus it shows poor current responses. TEOS used in this study provided strong Si-O-Si bonds with the treated ITO glass, which effectively prevents the sensor film from flake off.

The use of the dip coater in this study, at a constant rate is to form a thin uniform film. Thickness of film is one of the most effective factors that affect the sensitivity of the MIP sol-gel hybrid film (Firenman-Shoresh *et al*., 2005). Although thicker film would increase the amount of methamidophos imprinted onto the sol-gel hybrid film, however it will slow the penetration of methamidophos towards the electrode and delay the detection time. Therefore, in this study, the dip coating process was performed only once. The thickness of the film obtained was ~149 nm.

3.2 Characterisation and Evaluation of Molecularly Imprinted Sensor

The blocking/insulating properties of the MIP sol-gel hybrid film (methamidophos template removed and unremoved) was studied in the presence of $[Fe(CN)_6]^{3-}/[Fe(CN)_6]^{4-}$ redox couple measurement in the potential range from -0.2 V to +0.6 V to ensure that the sol-gel hybrid film has successfully be imprinted with the methamidophos template when there are cavities produced and allowed the penetration of $[Fe(CN)_6]^{3-}/[Fe(CN)_6]^{4-}$ ions from the electrolyte towards the working electrode (Hu *et al*., 2012; Sharma *et al*., 2012). Bare gold (Au), glassy carbon electrode (GCE) and ITO glass were used as reference working electrode in the blocking/insulating properties study. The $[Fe(CN)_6]^{3-}/[Fe(CN)_6]^{4-}$ redox peaks observed using reference electrodes were compared with the new developed working electrode. Cyclic voltammogram at the Au, GCE and ITO glass showed a relatively well defined redox peaks with peak potential difference (ΔE_p) of 221, 361 and 171 mV, respectively. The peak potential of GCE is highest among the three electrodes (Figure 1a), which may be contributed to the slow kinetics of the electron transfer on carbon (Liu *et al*., 2005). In Figure 1b, redox peaks were recorded using a reference NIP and the MIP sol-gel hybrid CNPrTEOS film (methamidophos template removed and unremoved). A couple of similar redox peaks of $[Fe(CN)_6]^{3-}/Fe(CN)_6]^{4-}$ as when using reference electrodes were observed using the MIP sol-gel hybrid CNPrTEOS film after

removal of methamidophos template. This suggested that MIP sol-gel hybrid CNPrTEOS film had successfully been synthesized on the ITO glass surface and cavities were produced in the MIP sol-gel hybrid CNPrTEOS film as a result of the template methamidophos removal (Fang *et al*., 2009; Huang *et al*., 2011). No response could be observed with both the NIP ITO glass and MIP sol-gel hybrid CNPrTEOS-coated ITO glass (before methamidophos template removal). The result shows that the NIP film and methamidophos template on MIP film have retarded the electron transfer between the electrolyte and the electrode. There is no difference in the cyclic voltammograms obtained in the presence or absence of methamidophos template, indicating that methamidophos does not exhibit any electroactivity in the potential range chosen (-0.2V to +0.6V).

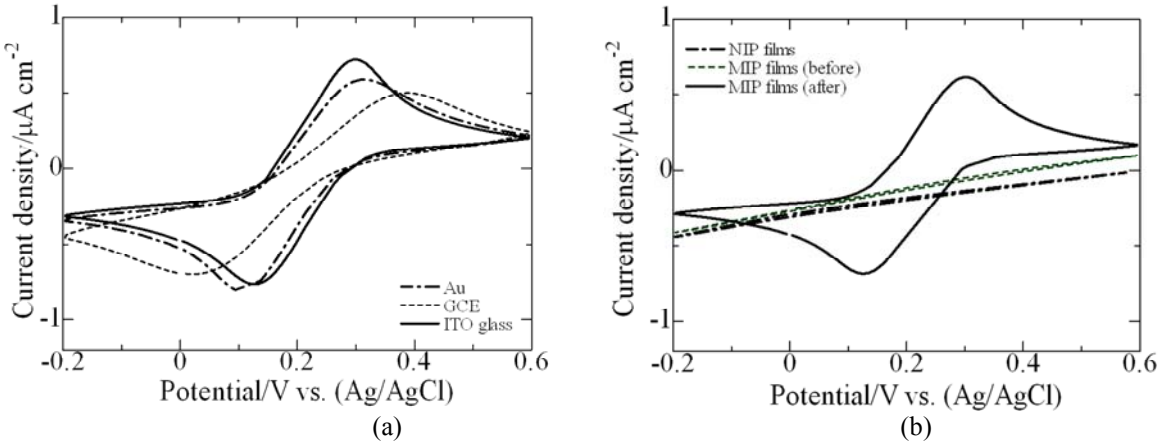


Figure 1: Cyclic voltammogram of 0.01M $K_3[Fe(CN)_6]$ in 0.10 M KCl using (a) reference bare gold, glassy carbon electrodes and ITO glass and (b) reference NIP sol-gel hybrid CNPrTEOS-coated ITO glass substrate, MIP sol-gel hybrid CNPrTEOS-ITO glass electrodes before and after removal of methamidophos template.

FE SEM was applied to characterise the surface morphology of the sol-gel hybrid film-coated ITO glass. From Figure 2, both films shows smooth surface when characterized at low magnification (×50K). Higher magnification at ×100K shows that the surface of MIP sol-gel hybrid film, before undergo the desorption process in ethanol under ultrasonic irradiation, are uniformly and homogenously disperse MIP sol-gel hybrid particles (Figure 2a) while Figure 2b shows cavities caused by the removal of methamidophos template. These cavities can selectively bind with the target molecules (methamidophos) and allow them to penetrate freely.

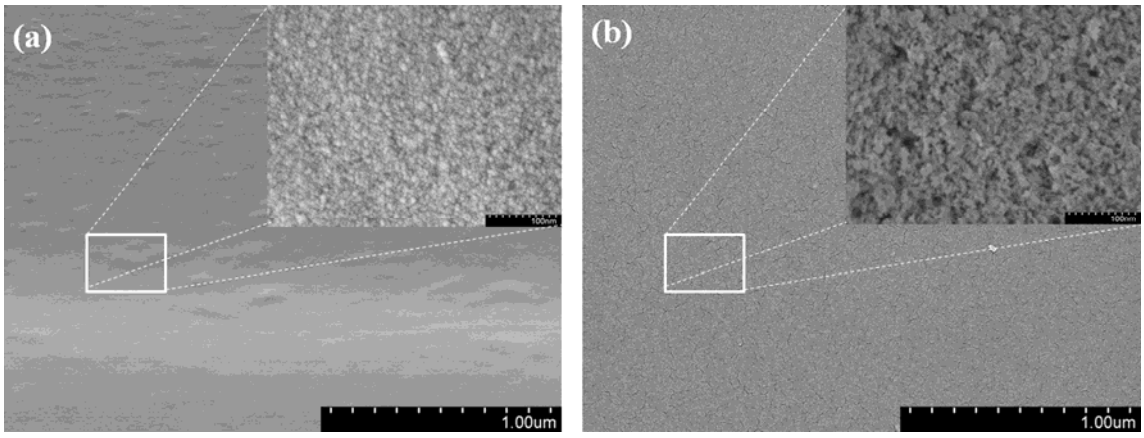


Figure 2: FE SEM micrographs of MIP sol-gel hybrid CNPrTEOS surfaces for (a) before (magnification: ×50K and ×100K) and (b) after template removal (magnification: ×50K and ×100K).

3.3 Electrochemical Detection of Methamidophos

Figure 3 illustrates the CV responses for increasing methamidophos concentration in 0.05 M PBS (pH 7.0) containing 0.1 M KCl. The linear range, limit of detection (LOD) (S/N=3) and standard deviation for methamidophos using MIP sol-gel hybrid CNPrTEOS were 0.5 to 10 pg mL^{-1}, 0.25 pg mL^{-1} (part-per-trillion) and 4.04% (n = 7), respectively. The detection limit achieved is very important to detect ultra trace level of pesticides in samples with complex matrix.

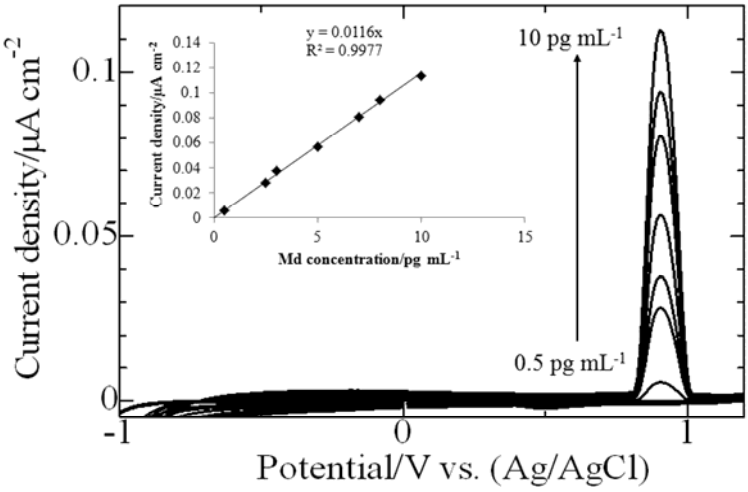


Figure 3: Cyclic voltammograms of increasing methamidophos concentration in 0.05 M PBS (pH = 7) containing 0.1 M KCl. The inset shows the calibration curve of methamidophos. Methamidophos concentration was 0.5, 2.5, 3.0, 5.0, 7.0, 8.0, 10.0 pg mL^{-1}, respectively. Scan rate: 100 mV s^{-1}.

4. CONCLUSION

This work demonstrated a sensitive, rapid and simple electrochemical sensor for detection of polar organophosphate chemical warfare agent which was successfully developed by using sol-gel hybrid molecular imprinted technology. Analysis of polar analyte is challenging as they are soluble in water and polar solvent. The ability of the synthesized sol-gel hybrid CNPrTEOS Md MIP film as an electrochemical sensor for the detection of methamidophos was successfully demonstrated. Sol-gel hybrid CNPrTEOS as functional monomer for methamidophos recognition was coated onto the ITO glass substrates and significantly exhibited excellent sensitivity and selectivity for the template molecule rebinding. Under selected analytical conditions, the electrochemical sensor shows very low detection limit down to part per trillion level (pg mL^{-1}) which seems to be a promising tool for trace-level detection of organophosphate chemical warfare agent. Alternatively, the preparation of MIP sol-gel hybrid CNPrTEOS-coated ITO glass for other template molecules could be also easy with the procedure described in this study.

ACKNOWLEDGEMENT

Financial support from the Ministry of Science, Technology and Innovation (MOSTI), Malaysia for the National Science Fellowship (NSF) received by the first author is gratefully acknowledged. We also would like to thank Toyohashi University of Technology (TUT) and the Science & Technology Research Institute for Defence (STRIDE) for their support. Valuable discussions and support from Assoc. Prof. Hiroyuki Muto and Dr. Go Kawamura from TUT are highly acknowledged.

REFERENCES

Atta, N. F. & Abdel-Mageed, A. M. (2009). Smart electrochemical sensor for some neurotransmitters using imprinted sol-gel films. *Talanta*. **80**: 511-518.

Bismuth, C., Borron, S. W., Baud, F. J. & Barriot, P. (2004). Chemical weapons: documented use and compounds on the horizon. *Toxicol. Lett*. **149**: 11-18.

Black, R. M., Clarke, R. J., Read, R. W. & Reid, M. T. (1994). Application of gas chromatography-mass spectrometry and gas chromatography-tandem mass spectrometry to the analysis of chemical warfare samples, found to contain residues of the nerve agent sarin, sulphur mustard and their degradation products. *J. Chromatogr. A*. **662**: 301-321.

Diaz, J. A., Daley, P., Miles, R., Rohrs H. & Polla, D. (2004). Integration test of a miniature ExB mass spectrometer with a gas chromatograph for development of a low-cost, portable, chemical-detection system. *Trends Anal. Chem*. **4**: 314–321.

Fang, C., Yi, C., Wang, Y., Cao, Y. & Liu, X. (2009). Electrochemical sensor based on molecular imprinting by photo-sensitive polymers. *Biosens. Bioelectron*. **24**: 3164-3169.

Firenman-Shoresh, S., Turyan, I., Mandler, D., Avir, D. & Marx, S. (2005). Chiral electrochemical recognition by very thin molecularly imprinted sol-gel films. *Langmuir*. **21**: 7842-7847.

Gao, N., Xu, Z., Wang, F. & Dong, S. (2007). Sensitive biomimetic sensor based on molecular imprinting at functionalized indium tin oxide electrodes. *Electroanalysis*. **19**: 1655-1660.

Haas, R. (1998). Determination of chemical warfare agents: Gas chromatographic analysis of chlorovinylarsines (Lewisite) and their metabolites by derivatization with thiols (2^{nd} communication. *Environ. Sci. Pollut. Res. Int*. **5**: 2-3.

Huang, J., Zhang, X., Lin, Q., He, X., Xing, X., Huai, H., Lian, W. & Zhu, H. (2011). "Electrochemical sensor based on imprinted sol-gel and nanomaterials for sensitive determination of bisphenol A. *Food Control*. **22**: 786-791.

Hu, Y., Zhang, Z., Li, J., Zhang, H., Luo, L. & Yao, S. (2012). Electrochemical imprinted sensor for determination of oleanic acid based on poly (sodium 4-styrenesulfonate-co-acrylic acid)-grafted multi-walled carbon nanotubes-chitosan and cobalt hexacyanoferrate nanoparticles. Biosens. *Bioelectron*. **31**: 190-196.

Hu, Y., Zhang, Z., Zhang, H., Luo, L. & Yao, S. (2012). "Selective and sensitive molecularly imprinted sol-gel film-based electrochemical sensor combining mercaptoacetic acid-modified PbS nanoparticles with Fe_3O_4@Au-multi-walled carbon nanotubes-chitosan. *J. Solid State Electrochem*. **16**: 857-867.

Kern, W. & Puotinen, D. A. (1970). Cleaning solutions based on hydrogen peroxide for use in silicon semiconductor technology. *RCA Rev*. **31**: 187-206.

Kimm, G. L., Hook, G. L. & Smith, P.A. (2002). Application of headspace solid-phase microextraction and gas chromatography-mass spectrometry for detection of the chemical warfare agent bis(2-chloroethyl) sulfide in soil. *J. Chromatogr. A*. **971**: 185-191.

Li, C., Wang, C., Guan, B., Zhang, Y. & Hu, S. (2005). Electrochemical sensor for the determination of parathion based on *p-tert*-Butylcalix[6]-arene-1,4-crwon-4 sol-gel film and its characterization by electrochemical methods. *Sens. Actuators B*. **107**: 411-417.

Li, C., Zhan, G., Ma, M. & Wang, Z. (2012). Preparation of parathion imprinted polymer beads and its applications in electrochemical sensing. *Colloids Surf. B*. **90**: 152-158.

Li, H., Wang, Z., Wu, B., Liu, X., Xue, Z., & Lu, X. (2012). Rapid and sensitive detection of methyl-parathion pesticide with an electropolymerized, molecularly imprinted polymer capacitive sensor. *Electrochim. Acta*. **62**: 319-326.

Liu, G. Z., Liu, J. Q., Böcking, T., Eggers, P. K. & Gooding, J. J. (2005). The modification of glassy carbon and gold electrodes with aryl diazonium salt: The impact of the electrode substrate on the rate of heterogeneous electron transfer. *Chem. Phys*. **319**: 136-146.

Marx, S., Zaltsman, A., Turyan, I. & Mandler, D. (2004). Parathion sensor based on molecularly imprinted sol-gel films. *Anal. Chem*. **76**: 120-126.

Nassar, A.E., Lucas S.V. & Hoffland, L.D. (1999). Determination of chemical warfare agent degradation products at low-part-per-billion levels in aqueous samples and sub-part-per-million levels in soild using capillary electrophoresis. *Anal. Chem*. **71**: 1285-1292.

Newmark, J. (2004). Therapy for nerve agent poisoning. *Arch. Neurol*. **61**: 649-652.
Nozaki, H. & Aikawa, N. (1995). Sarin poisoning in Tokyo subway. *Lancet*. **345**: 1446-1447.
Patel, A. K., Sharma, S. & Prasad, B. B. (2009). Electrochemical sensor for uric acid based on a molecularly imprinted polymer brush grafted to tetraethoxysilane derived sol–gel thin film graphite electrode. *Mater. Sci. Eng. C*. **29**: 1545-1553.
Wada, T., Nagasawa E. & Hanaoka, S. (2006). Simultaneous determination of degradation products related to chemical warfare agents by high-performance liquid chromatography/mass spectrometry. *Appl. Organomet. Chem*. **20**: 573-579.
Wang, H., Lee, W.M., Shuang, S. & Choi, M.M.F. (2008). SPE/HPLC/UV studies on acrylamide in deep-fried flour-based indigenous Chinese food. *Microchem. J*. **89**: 90-97.
Xie, C., Li, H., Li, S., Wu, J. & Zhang, Z. (2010). Surface molecular self-assembly for organophosphate pesticide imprinting in electropolymerized poly(p-aminothiophenol) membranes on a gold nanoparticle modified glassy carbon electrode. *Anal. Chem*. **82**: 241-249.
Yang, Q., Sun, Q., Zhou, T., Shi, G. & Jin, L. (2009). Determination of parathion in vegetables by electrochemical sensor based on molecularly imprinted polyethyleneimine/silica gel films. *J. Agric. Food Chem*. **57**: 6558-6563.
Sharma, P. S., Pietrzyk-Le, A., D'Souza, F. & Kutner, W. (2012). Electrochemically synthesized polymers in molecular imprinting for chemical sensing. *Anal. Bioanal. Chem*. **402**: 3177-3204.
Shustak, G., Marx, S., Turyan, I. & Mandler, D. (2003). Application of sol-gel technology for electroanalytical sensing. *Electroanalysis*. **15**: 398-408.

A REVIEW OF TECHNIQUES FOR THE DETECTION OF BIOLOGICAL WARFARE AGENTS

Gian Marco Ludovici[1], Valentina Gabbarini[1], Orlando Cenciarelli[1,2*], Andrea Malizia[1,2], Annalaura Tamburrini[1], Stefano Pietropaoli[3], Mariachiara Carestia[1,2], Michela Gelfusa[2], Alessandro Sassolini[2], Daniele Di Giovanni[1,2], Leonardo Palombi[1,4], Carlo Bellecci[1,2] & Pasquale Gaudio[1,2]

[1]International Master Courses in Protection Against CBRNe Events, Department of Industrial Engineering - School of Medicine and Surgery, University of Rome Tor Vergata, Italy
[2]Department of Industrial Engineering, University of Rome Tor Vergata, Italy
[3]Department of Science, University of Rome 3, Italy
[4]Department of Biomedicine and Prevention, School of Medicine and Surgery, University of Rome Tor Vergata, Italy

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

ABSTRACT

Biohazards represent an important issue in the field of security, both for the destructive potential and the psychological, economic and social impact that the use of biological agents for biowarfare could have on populations. Early identification of an intentional biological event is essential to ensure correct management and response to the emergency. Much effort for the development of innovative equipment that permit prompt and remote detection of biological warfare agents are needed to achieve this goal. In this work, the different detection systems suitable in the CBRN context for biological agents will be analyzed, focusing on non-specific and specific point-detection systems, and stand-off detection systems, evaluating the pros and cons of each technology.

Keywords: *Biological warfare agents; non-specific and specific point-detection systems; stand-off detection systems; sensitivity and specificity; quickness of response.*

1. INTRODUCTION

In the last few decade, concerns on intentional use of biological agents (bacteria, viruses, fungi, toxins) as weapons have increased along with the terrorism global alert. Among the non-conventional threats, biohazards is considered as an extremely demanding challenge for chemical, biological, radiological and nuclear (CBRN) experts, due to difficulties concerning detection and identification of biological agents (Cenciarelli *et al.*, 2013a), and lack of suitable prophylactic and therapeutic measures for many of these pathogens. Biohazards are caused from the dispersion in the environment of a microorganism or toxin, with the consequent possibility to cause a communicable disease in affected people (except for toxins, which are not infectious). Such an event could occur through natural spread of an infectious disease (i.e., influenza epidemics or the ongoing Ebola virus disease outbreak in West Africa), accidental dispersion of an agent (i.e., an accident in a laboratory where biological agents are usually used), or intentional dissemination as a terrorist act (Cenciarelli *et al*., 2013b, 2014a).

Biological warfare refers to the deliberate use of microorganisms and toxins, generally of microbial, plant or animal origin, to produce diseases in humans, animals and plants (DaSilva, 1999). The intentional release of aggressive biological agents aims to strike a large number of people, causing serious illnesses and increasing their spread. Biological weapons (except toxins) have, in fact, an intrinsic characteristic; they are able to multiply in a host organism and be transmitted to others, thereby causing unpredictable effects in the population, both in terms of victims and geographical spread (Rotz *et al*., 2002). Easy dissemination and high lethality of some biological agents (CDC, 2015) make it difficult for prompt detection and identification of a biological attack (Cenciarelli *et al.*, 2013a). Biological agents can remain undetected for hours, days or even weeks before the onset of the illness. Without any immediate sign of dissemination (as occurred in the event of anthrax letters) and before disease confirmation by health authorities through clinical tests, a biological event can only be identified by monitoring systems. Great importance should be addressed to this aspect because while tools for immediate detection of chemical and radiological agents are largely available (Jopling, 2005; Sferopoulos, 2009), preparedness towards biological agents is still low, with just some rare exceptions (Kaszeta, 2012; Cenciarelli *et al.*, 2013a). Traditional methods for detection and identification of biological agents lack the speed and sensitivity to be applied in the field because they cannot provide results in real time (Iqbal *et al*., 2000).

Detection systems must be highly sensitive, being able to detect extremely limited amounts of biological particles. For example, a concentration of 100 particles/L of *Bacillus anthracis* or only 10 particles/L of *Francisella tularensis* can infect a person (Primmerman, 2000). Moreover, such a system should be able to discriminate pathogens from other harmless biological and non-biological components that are part of the environmental background (e.g. diesel particulates, pollen, dust), to achieve a low false-positive rate. Normally, ambient particle concentration exceeds the predetermined detection concentration of biological agents (Greenwood *et al*., 2009). A further quality that must be evaluated is the quickness of response, because prompt detection is the key for an efficient intervention (Primmerman, 2000). These requirements make it very easy to understand how hard it is to develop detection systems that allow for effective detection of biological agents.

It must be considered that some promising tools for detection of biological agents have been developed and tested, especially by the army. However, they are complex systems, the use of which requires special formations for their proper execution and maintenance. Moreover, they tend to be very expensive. In recent years, many companies have focused their attention on the development of biodetection tools that are less expensive and easier to use than the products of military source (Ozanich *et al*., 2014).

Detection systems can be divided into two broad categories; point-detection and stand-off detection systems. Point-detection systems are able to sense biological particles in a short range (from centimeters to some meters), while stand-off detection systems have the capability to detect biological particles from far away, even for some kilometers (Švábenská, 2012).

In this paper, several technologies for the biological agents detections in the CBRN context were investigated, evaluating both non-specific and specific point-detection systems and remote (stand-off) detection systems; for each system advantages and disadvantages were assessed.

2. POINT-DETECTION SYSTEMS

Point-detection systems may be specific or non-specific, depending on their ability to discriminate a definite biological agent once the analysis is performed. Non-specific detection systems are only able to determine if a biological agent is present, without providing any identification. On the other hand, specific point-detection systems are able to return an identification of the biological agent.

2.1 Non-Specific Point-Detection Systems

- **Particle sizers'** operating principle is based on counts of the relative number of particles included in a predetermined size range (typically 0.5-30 μm) (Pazienza *et al*., 2014). One of the most diffused particle sizers is High Volume Aerodynamic Particle Sizer (HVAPS), in which particles are exposed to a constant flow of concentrated air. Within the aerosol, particles will accelerate with different rates, depending on their size. Thus, the acceleration will be higher for smaller particles. This technology, due to a laser measuring device, provides information about the number, size and distribution of particles. However, such device does not permit distinction among biological and non-biological aerosols.

- **Fluorescence based systems** exploit the properties of endogenous fluorophores to detect biological agents through bioluminescence (Carestia *et al.*, 2014). This method consists of the excitation of molecular components widely present in biological materials (such as the aromatic aminoacid tryptophan) with light beams (usually in the ultraviolet (UV) spectrum). With the light emission after excitation, these approaches could be used for non-specific detection of biological agents in unknown samples exploiting emission of a common fluorophore. Among the detectors that use fluorescence measurements, the most prominent is Fluorescent Aerodynamic Particle Sizer (FLAPS) (Figure 1). It is an aerodynamic particle sizer, like the above-mentioned HVAPS, provided with an additional UV laser. A variant of FLAPS is Ultra Violet Aerodynamic Particle Sizer (UVAPS) that uses, for sizing, the particles time of flight, light dispersion and UV fluorescence intensity to detect biological agents in air samples. Unlike FLAPS and UVAPS, Biological Aerosol Warning System (BAWS) technology does not provide a count of particles, but can detect in real time and discriminate particles of biological agents from other airborne particles naturally present as environmental background (Huffmann *et al*., 2013).

- **Viable particle size samplers (impactors)** operate by accelerating an air flow through a nozzle before deflecting it against an impact surface maintained at a fixed distance. Larger particles that are not able to follow the flow due to their inertia will be separated from smaller particles. Small particles exit the sampler, passing through distinct stages, each one containing progressive dimension holes that allow the diffusion of particles according to their size and the collection on a specific surface. The collection plate is generally represented by a Petri dish containing selective agar to allow the growth of specific microorganisms. After an incubation period, typically 24-48 h, the number of colonies grown on each plate is evaluated (Xu *et al*., 2013).

Figure 1: Schematic representation of a Fluorescent Aerodynamic Particle Sizer (FLAPS).
(Adapted from http://www.tsi.com)

- **Virtual impactors** represent a class of tools similar to the viable particle size samplers, except for the collection plate, which consists of a probe that the larger particles can penetrate. Moreover, once reaching the final stage, particles will flow into a liquid matrix, with the production of a highly concentrated liquid sample. The BioVIC aerosol collector is a device able to pre-concentrate the flow of air, by suspending a large number of particles in a reduced volume of liquid, in a small flow of air or on a solid surface for subsequent detection by a sensor. It can be associated with polymerase chain reaction (PCR) technology, optical fluorescence-based sensors, mass spectrometry or flow cytometry. An evolution of BioVIC is the BioCapture BT-500 air sampler (Figure 2), which is a portable instrument that collects airborne samples to quantify the particulate concentration. Pathogens are collected and concentrated in a liquid sample for further analysis carried out through the rapid identification of cellular components, nucleic acids or other identifiable components in liquid matrix (Kesavan *et al*., 2011).

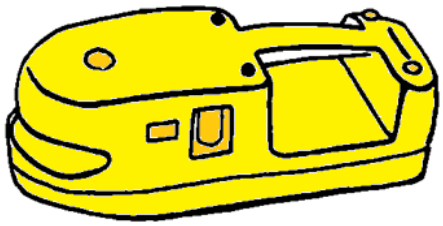


Figure 2: Schematic representation of a BioCapture BT-500 air sampler.
(Redrawn and adapted from http://www.htds.fr)

2.2 Specific Point-Detection Systems

- **Molecular biology techniques**, including PCR, is the most common method to amplify small amounts of genetic material), allowing for the detection of biological agents (bacteria, bacteria spores or viruses only; toxins do not possess genome) (Iqbal *et al*., 2000). The main limitation to this technique is the requirement for a prior knowledge of the biological

agent analyzed, due to the need of specific primer sequence for the nucleic acid amplification. In addition, each reaction is generally specific for a single agent, except for multiplex PCR, by which the analysis of several agents at once is possible (Greenwood *et al*., 2009). Specific probes may be applied as a complement to the PCR. This technique detects the presence of a specific gene sequence in the sample, by exploiting the interaction among complementary sequences. Nowadays, such an approach finds common application in DNA microarrays (Lee *et al*., 2008; Splettsosser *et al*., 2010), based on the simultaneous hybridization of thousands of specific gene sequences. Briefly, different DNA sequences are deposited at a distance of a few hundred microns on a chip, usually made of glass, consisting of an array of microscopic DNA probes. The hybridization process is highly selective, specific and sensitive. A large number of target sequences will be available on a single support, potentially providing more complete information than that of a simple PCR, although depending on it for signal intensity (Call *et al*., 2003). However, providing increased information per unit time is not the only advantage offered by microarrays. A significant reduction in the time of analysis, small sample volume and reagents required are other important elements in favor of this technique (Ivnitski *et al*., 2003).

- **Flow cytometry** evaluates both the physical and chemical features of an air flow when it runs through a testing point. This instrument counts and measures the size of particles dispersed after liquid phase concentration using a laser diffraction system. Generally, a fluorescent dye that reacts with biological components, such as DNA, is added to the sample before the measurements. Flow cytometers are very complex systems provided with sophisticated mechanisms that permit the analysis of thousands of cells in a few seconds. Among these, Mini-Flow Cytometer and Fluorescence Activated Cell Sorting (FACS) Caliber (Becton Dickinson) are the most commonly used.

- **Mass spectrometry** is an analytical technique that provides information about structure and molecular weight of biological agents requiring minimal samples amounts (order of nanograms). Generally, it is applied in combination with separating techniques, such as gas chromatography and High-Performance Liquid Chromatography (HPLC) (Figure 3) and works by ionizing molecules to generate molecule fragments, whose pattern constitutes the mass spectrum, which is a plot of the ion signal as a function of the mass-to-charge ratio. This technique requires samples in gaseous state. Examples of such tools are Matrix-Assisted Laser Desorption Ionization-Time of Flight-Mass Spectrometry (MALDI-TOF-MS) and Chemical Biological Mass Spectrometer (CBMS) (Figure 4) (Wieser *et al*., 2012; Laskay *et al*., 2012).

- **Immunoassay technologies** allow for the identification of biological agents using the specific binding of antigens with specific antibodies forming a detectable complex (Peruski & Peruski, 2003). Generally, these assays provide a response in a short time. Their sensitivity can vary depending on the sample medium, suspected agent and specific device (Greenwood *et al.*, 2009). Hand-Held Immunochromatographic Assays (HHAs) are disposable kits that, working on the principle of antigen/antibody interaction, show their results colorimetrically, with the same mechanism of a pregnancy test. They can provide both qualitative and semiquantitative response about a specific agent. These devices are

very easy to use and have found important application during the anthrax emergency (Biagini *et al*., 2006), being suitable in screening practices. However, they show some limitations, among which the possibility to detect only one agent per assay strip, implying that several hand-held devices must be used to identify the presumptive agent. Moreover, the quantitative response is limited to the human eye that has to perceive the colorimetric intensity of the outcome (Peruski & Peruski, 2003). Other immunoassays technologies exploit biosensor approaches that utilize fluorescence properties to detect biological agents. For example, Fiber Optic Wave-Guide (FOWG) uses optical fiber probes coated with antibodies and a fluorescent reporter antibody to assess the presence of a suspected agent (Wandermur *et al*., 2014). The antibodies used in immunoassays must be selected with care, because their affinity and specificity represent the limiting factors for these technologies (Peruski & Peruski, 2003).

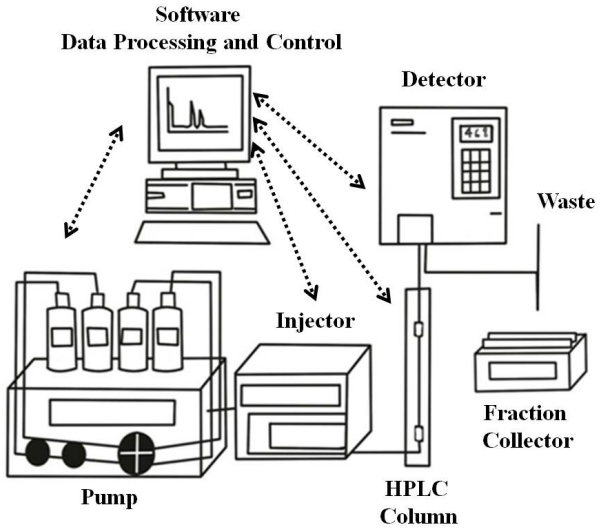


Figure 3: Schematic representation of High-Performance Liquid Chromatography (HPLC).
(Adapted from http://www.ebah.com.br)

Figure 4: Schematic representation of a Chemical Biological Mass Spectrometer (CBMS).
(Adapted from http://doctrine.vavyskov.cz)

3. STAND-OFF DETECTION SYSTEMS

Stand-off technologies are designed to detect biological agents remotely with respect to the point of release. One of the technologies more suitable for this purpose is based on Light Detection and Ranging (LIDAR) systems (Figure 5). LIDAR technology is based on a short laser pulse transmitted through the atmosphere. A part of the emitted radiation is reflected by atmospheric particles such as molecules, aerosols, pollen or dusts (Cenciarelli *et al*., 2014b). Since LIDAR systems use light signals consisting of energy at short wavelength, they are able to identify small aerosol particles (< 20 μm in diameter) such as biological agents. LIDAR can also use wavelengths in the infrared (IR) spectrum, so it is able to reach distances of several kilometers (Carestia *et al*., 2014). However, using IR spectrum, LIDAR is not able to discriminate biological agents from non-biological aerosols, and, for this reason, the use of Laser Induced Fluorescence (LIF) technology, which uses light beams of the UV wavelength, represents the best choice to conjugate detection capability to long range (up to 1 km). Thus, UV-LIF (Warren *et al.*, 2004) is a promising technique to allow fast stand-off detection and gross discrimination between biological agents and background noise, taking advantage of the intrinsic fluorescence of biological molecules. UV-LIF technology can find wider use at night or in low atmospheric light conditions, while the diurnal bright background significantly reduces its ability of detection (Buteau *et al*., 2013).

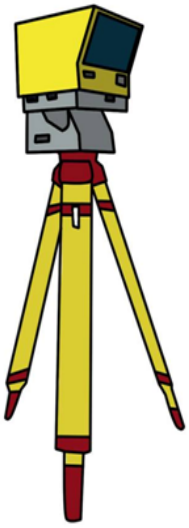


Figure 5: Schematic representation of a Light Detection and Ranging (LIDAR). (Adapted from http://al.water.usgs.gov)

In addition to the problem of distinguishing between hazardous from naturally-occurring biological agents, issues on the distinction between organic and inorganic aerosols evidently affect the stand-off systems that are currently available or under development. Among them, the Micropulse Lidar (MPL) 1000 IR-LIDAR system, developed by Scientific and Engineering Student Internship Program (SESI) in collaboration with National Aeronautics and Space Administration (NASA), is the most likely to be used as a reliable system for remote detection (Givens *et al*., 2012). A more ambitious device is the hybrid IR/UV system, Hybrid LIDAR, developed under the sponsorship of Defense Advanced Research Projects Agency (DARPA), whose objective is the development of a system mounted on an unmanned aerial vehicle (UAV), thus able to act autonomously for analyzing suspicious clouds using LIF technology (Perez *et al*., 2012).

In recent years, many efforts have been focused on the development of an even more efficient UV-LIF system and the creation of a LIDAR system suitable for detection of biological warfare agents, exploiting the intrinsically fluorescent molecular components presents in all biological agents (Hsu *et al*., 2012). However, it must be considered that the detection of biological warfare agents through fluorescence measurements is often complicated by interference from non-biological aerosols containing aromatic hydrocarbons (for example due to industrial processes and smog), as well as by biological aerosols constituting environmental background, such as pollen, fungi and bacteria (Healy *et al*., 2014).

4. CONCLUSION

Early detection of intentional diffusion of a biological agent is essential for effective intervention. Although several point detection technologies are currently available for the detection of biological agents, discrimination between microorganisms deliberately released and particles naturally present in the environmental background is extremely challenging because harmless and pathogenic biological agents often only differ at the molecular level.

To date, the identification of biological warfare agents is possible with just a few point-detection strategies, while some remote methods are under research. Point and stand-off detectors should be networked to give integrated information to experts in CBRN events, in order to promptly face any emergency (Primmerman, 2000; Ivnitski *et al*., 2003).

Several international research groups are focusing their attention on the study of stand-off detection systems for the identification of biological agents through UV-LIF technology. However, they are still in a preliminary phase of development. Thus, many resources must be invested to optimize systems that are able to detect possible bioterrorist attacks and to identify the biological agents involved in it. This can also be done through the implementation and refinement of already existing technologies, such as a database of spectral signature of each biological agent.

ACKNOWLEDGMENT

Special acknowledgement for the realization of this work goes to the International Master Courses in Protection Against CBRNe Events (http://www.mastercbrn.com). The first two authors provided equal contribution to this paper.

REFERENCES

Biagini, R.E., Sammons, D.L., Smith, J.P., MacKenzie, B.A., Striley, C.A., Snawder, J.E., Robertson, S.A. & Quinn, C. P. (2006). Rapid, sensitive, and specific lateral-flow immunochromatographic device to measure anti-anthrax protective antigen immunoglobulin g in serum and whole blood. *Clin. Vaccine Immunol.*, **13**:541-546.

Buteau, S., Simard, J.R., Roy, G., Lahaie, P., Nadeau, D. & Mathieu, P. (2013). Standoff detection of bioaerosols over wide area using a newly developed sensor combining a cloud mapper and a spectrometric LIF lidar. *SPIE Security + Defence* 890109-890109, International Society for Optics and Photonics (SPIE), Bellingham, Washington.

Call, D.R., Borucki, M.K., & Loge, F.J. (2003). Detection of bacterial pathogens in environmental samples using DNA microarrays. *J. Microbiol. Method.*, **53**:235-243.

Carestia, M., Pizzoferrato, R., Cenciarelli, O., D'Amico, F., Malizia, A., Gelfusa, M., Scarpellini, D. & P. Gaudio. (2014). Fluorescence measurements for the identification of biological agents features for the construction of a spectra database. *2014 Fotonica AEIT Ital. Conf. Photon. Technol. (Fotonica AEIT 2014)*, 12-14 May 2014, Naples, Italy, pp. 1-4.

Cenciarelli, O. Pietropaoli, S, Frusteri, L., Malizia, A., Carestia, M., D'Amico, F., Sassolini, A., Di Giovanni, D., Tamburrini, A.,Palombi, L., Bellecci, C. & Gaudio, P. (2014a). Biological emergency management: the case of Ebola 2014 and the air transportation involvement. *J. Microb. Biochem. Technol.*, **6**:247-253.

Cenciarelli, O., Pietropaoli, S., Gabbarini, V., Carestia, M., D'Amico, F., Malizia, A., Gelfusa, M., Pizzoferrato, R., Sassolini, A., Di Giovanni, D., Orecchio, F.M., Palombi, L., Bellecci, C., & Gaudio, P. (2014b). Use of Non-Pathogenic Biological Agents as Biological Warfare Simulants for the Development of a Stand-Off Detection System. *J. Microb. Biochem. Technol.*, **6**: 375-380.

Cenciarelli, O., Malizia, A., Marinelli, M., Pietropaoli, S., Gallo, R., D'Amico, F., Bellecci, C., Fiorito, R., Gucciardino, A., Richetta, M., & Gaudio, P. (2013a). Evaluation of biohazard management of the Italian national fire brigade. *Defence S&T Tech. Bull.,***6**:33-41.

Cenciarelli, O., Rea, S., Carestia, M., D'Amico, F., Malizia, A., Bellecci, C., Gaudio, P., Gucciardino, A. & Fiorito, R. (2013b). Bioweapons and bioterrorism: A review of history and biological agents. *Defence S&T Tech. Bull.*, **6**:111-129.

Centers for Diseases Control and Prevention (CDC). 2015. *Bioterrorism Agents / Diseases*. Available online at: http://www.bt.cdc.gov/agent/agentlist-category.asp (Last access date: February 16, 2015).

DaSilva, E. (1999). Biological warfare, bioterrorism, biodefence and toxin weapons convention. *EJB*, **2**:99-129.

Givens, R.N., Walli, K.., & Eismann, M. T. (2012). Fusion of LIDAR data with hyperspectral and high-resolution imagery for automation of DIRSIG scene generation. IEEE Appl. Imagery Pattern Recogn. Workshop (AIPR), 9-11 October 2012, Cosmos Club, Washington DC, pp.1-7.

Greenwood, D.P., Jeys, T.H., Johnson, B., Richardson, J.M., & Shatz, M.P. (2009). Optical techniques for detecting and identifying biological-warfare agents. *Proc. IEEE*, **97**:971-989.

Healy, D.A., Huffman, J.A., O'Connor, D.J., Pöhlker, C., Pöschl, U., & Sodeau, J.R. (2014). Ambient measurements of biological aerosol particles near Killarney, Ireland: a comparison between real-time fluorescence and microscopy techniques. *Atmos. Chem. Phys.*, **14**:8055-8069.

Hsu, P.S., Kulatilaka, W.D., Jiang, N., Gord, J.R., & Roy, S. (2012). Investigation of optical fibers for gas-phase, ultraviolet laser-induced-fluorescence (UV-LIF) spectroscopy. *Appl. Optics*, **51**:4047-4057.

Huffmann, J.A., Prenni, A.J., DeMott, P.J., Pöhlker, C., Mason, R.H., Robinson, N.H., Fröhlich-Nowoisky, J., Tobo, Y., Després, V.R., Garcia, E., Gochis, D.J., Harris, E., Müller-Germann, I., Ruzene, C., Schmers, B., Sinha, B., Day, D.A., Andreae, M.O., Jimenez, J.L., Gallagher, M., Kreidenweis, S.M., Bertram, A.K., & Pöschl, U. (2013). High concentrations of biological aerosol particles and ice nuclei during and after rain. *Atmos. Chem. Phys.*, **13**:6151-6164.

Iqbal, S.S., Mayo, M.W., Bruno, J.G., Bronk, B.V., Batt, C.A., & Chambers, J.P. (2000). A review of molecular recognition technologies for detection of biological threat agents. *Biosensors Bioelectron.*, **15**:549-578.

Ivnitski, D., O Neil, D. J., Gattuso, A., Schlicht, R., Calidonna, M., & Fisher, R. (2003). Nucleic acid approaches for detection and identification of biological warfare and infectious disease agents. *Biotech.*, **35**:862-869.

Jopling, L. (2005). Chemical, biological, radiological or nuclear (CBRN) detection: a technological overview. *Special Report to NATO Parliamentary Assembly*, 167.

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

Kesavan, J. S., Schepers, D., & Bottiger, J. (2011). *Characteristics of Twenty-Nine Aerosol Samplers Tested at US Army Edgewood Chemical Biological Center (2000-2006) (No. ECBC-TR-822)*. Edgewood Chemical Biological Center, Aberdeen, Maryland.

Laskay, Ü., Kaleta, E.J., and Wysocki, V.H. (2012). Methods of mass spectrometry in homeland security applications. *In:* Lee, M.S. (Eds.), *Mass Spectrometry Handbook*. John Wiley & Sons, New York, pp. 419-439.

Lee, D.Y., Lauder, H., Cruwys, H., Falletta, P., & Beaudette, L.A. (2008). Development and application of an oligonucleotide microarray and real-time quantitative PCR for detection of wastewater bacterial pathogens. *Sci. Total Environ.*, **398**:203-211.

Ozanich, R.M., Baird, C.L., Bartholomew, R.A., Colburn, H.A., Straub, T.M., Bruckner-Lea, C.J. (2014). *Biodetection Technologies for First Responders: 2014 Edition*. Battelle Pacific Northwest National Laboratory, Richland, Washington.

Pazienza, M., Britti, M.S., Carestia, M., Cenciarelli, O., D'Amico, F., Malizia, A., Bellecci, C., Fiorito, R., Gucciardino, A., Bellino, M., Lancia, C., Tamburrini, A. & Gaudio, P. (2014).Use of particle counter system for the optimization of sampling, identification and decontamination procedures for biological aerosols dispersion in confined environment.*J. Microb. Biochem. Technol.*, **6**:43-48

Perez, P., Jemison, W.D., Mullen, L., and Laux, A. (2012). Techniques to enhance the performance of hybrid lidar-radar ranging systems. *Proc. IEEE OCEANS 2012 Conf.,* Virginia Beach, USA.

Peruski, A.H., & Peruski, L.F. (2003). Immunological methods for detection and identification of infectious disease and biological warfare agents. *Clin. Diagn. Lab. Immunol*. **10**: 506-513.

Primmerman, C.A. (2000). Detection of biological agents. *Lincoln Lab. J.*, **12**:1-32.

Rotz, L.D., Khan, A.S., Lillibridge, S.R., Ostroff, S.M., & Hughes, J.M. (2002). Public health assessment of potential biological terrorism agents. *Emerg. Infect. Dis.*, **8**:225-230.

Sferopoulos, R. (2009). *A Review of Chemical Warfare Agent (CWA) Detector Technologies and Commercial-Off-the-Shelf Items*. Human Protection and Performance Division DSTO Defence Science and Technology Organization Australia DSTO-GD-0570.

Splettstoesser, W.D., Seibold, E., Zeman, E., Trebesius, K., & Podbielski, A. (2010). Rapid differentiation of Francisella species and subspecies by fluorescent in situ hybridization targeting the 23S rRNA. *BMC Microbiol.*, **10**:72.

Švábenská, E. (2012).Systems for detection and identification of biological aerosols. *Defence Sci. J.*, **62**:404-411.

Wandermur, G., Rodrigues, D., Allil, R., Queiroz, V., Peixoto, R., Werneck, M., and Miguel, M. (2014). Plastic optical fiber-based biosensor platform for rapid cell detection. *Biosensor Bioelectron.*, **54**:661-666.

Warren, J.W., Thomas, M.E., Rogala, E.W., Maret, A.R., C. A. Schumacher, C.A., and Diaz, A. (2004). Systems engineering tradeoffs for a bio-aerosol lidar referee system. *Proc. SPIE Chem. Biol. Sens.*, **5416**:204–215.

Wieser, A., Schneider, L., Jung, J., and Schubert, S. (2012). MALDI-TOF MS in microbiological diagnostic – identification of microorganisms and beyond (mini review). *Appl. Microbiotechnol. Biotechnol.*, **93**:965-974.

Xu, Z., Wei, K., Wu, Y., Shen, F., Chen, Q., Li, M., & Yao, M. (2013). Enhancing bioaerosol sampling by andersen impactors using mineral-oil-spread agar plate. *PloS one*, **8**:e56896.

PERFORMANCE ANALYSIS OF A MINIMUM CONFIGURATION MULTILATERATION SYSTEM FOR AIRBORNE EMITTER POSITION ESTIMATION

Ahmad Zuri Sha'ameri*, Yaro Abdulmalik Shehu & Winda Asuti

Department of Electronic and Computer Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Malaysia

*E-mail: zuri@fke.utm.my

ABSTRACT

A multilateration system estimates the position of the airborne emitter (AE) of an aircraft by measuring the time-delay between the received signals. Provided the signal-to-noise ratio (SNR) is sufficiently high at above 34 dB, the multilateration system can accurately estimate position in 3D. This is an advantage over angle of arrival (AOA) that estimates position only in 2D. This paper investigates the position estimation (PE) coverage of a minimum receiver arrangement for a multilateration system operating at frequencies of 1,090 MHz and 8 to 12 GHz (X-band). Due to complexity of the PE estimation, a methodology is introduced based on Monte Carlo simulations to estimate the PE coverage. The coverage is evaluated at various SNR, range and bearing, and benchmarked with the International Civil Aviation Organization (ICAO) reduced vertical separation minimum (RVSM), Federal Aviation Administration (FAA) horizontal separation and performance of current air defence radar technology. The evaluation shows that the multilateration system is able to estimate position in 3D for a range of 20 km and at altitude of 15 km, and in 2D for a range of 80 km.

Keywords: *Multilateration; time delay of arrival (TDOA); position estimation (PE); reduced vertical separation minimum (RVSM); horizontal separation.*

1. INTRODUCTION

Multilateration is a surveillance technology to estimate the position of an aircraft by receiving the electromagnetic emissions –by transponder and radar- from multiple receiving stations (ICAO, 2007). Applications of the technology are in electronic warfare (EW) (Falk, 2004; Wiley, 2006), air traffic control (ATC) (ICAO, 2007) and regulatory organisations (Francis, 2011). In EW and regulatory organisations, multilateration is used to search, intercept, identify and locate sources of intentional and unintentional radiated electromagnetic energy (Falk, 2004). Wide area multilateration (WAM) (Neven *et al*., 2004) in ATC tracks aircrafts over en-route and approach area in the airspace. The system can also make use of positional messages provided by Automatic Dependent Surveillance Broadcast (ADS-B) transponders (ICAO, 2007) installed on board aircrafts.

There are two general approaches for position estimation (PE) of an airborne emitter (AE); time delay of arrival (TDOA) and angle of arrival (AOA) (Rohde & Schwarz, 2008). Many articles have described methods for estimating time delay (Gustafsson & Gunnarsson, 2003; Yushi & Abdulla Waleed, 2005; Wiley, 2006; Zhang & Xu, 2009; Dhull & Sahu, 2010; Mahdinejad & Seghaleh, 2013; Zhang *et al*., 2013). For example, Yushi & Abdulla Waleed (2005) used signal-to-noise ratio (SNR) as a benchmark to compare the performance of five different time delay estimation (TDE) techniques. Mahdinejad & Seghaleh (2013) provided a comparison between the different generalised cross correlation methods for TDE at different observation intervals to determine the accuracy and speed of estimation. The algorithm for PE is presented in Bucher & Misra (2002) and a synthesisable hardware description language model of 3D hyperbolic positioning system algorithm was implemented and simulated using IEEE numerical_std package. Besides TDE, many articles also focus on the application of multilateration as the next generation surveillance system to support existing

surveillance technologies, such as primary surveillance radar (PSR), secondary surveillance radar (SSR) and ADS-B (Neven *et al*., 2004; ICAO, 2007) in compliance to the International Civil Aviation Organization (ICAO) standards. In Neven *et al*. (2004), an overview of a multilateration system was performed based on the 1,090 MHz band and applied in a wide area surveillance environment.

This paper covers the deployment of multilateration systems, and evaluates PE errors in altitude and horizontal plane for various directions, ranges and frequency bands. First, the structure of the multilateration system is presented, followed by the methodology for PE errors and coverage. The simulation results are then presented, followed by discussions and finally, the conclusion.

2. MULTILATERATION SYSTEM STRUCTURE AND RECEIVED SIGNAL MODEL

The structure of the multilateration system is first described in this section followed by the frequency bands for the various types of signals relevant to this application.

2.1 Multilateration System Structure

A typical structure of a multilateration system is shown in Figure 1. It consists of multiple receivers that are spatially located and connected to a command centre. The command centre - the reference point in the 3D plane - derives the position of an AE that could be a fixed wing aircraft or rotary wing aircraft from its electromagnetic emission by estimating the TDOA between the receivers. The electromagnetic emission could come from the onboard transponder SSR, ADS-B and Identification, Friend or Foe (IFF) (or PSR). The capability to resolve the AE position in 2D or 3D depends on the number of receivers (Bucher & Misra, 2002). A minimum of four receivers is required for a PE of an AE (Neven *et al*., 2004). Through an averaging process, a larger number of receivers generally improves PE accuracy in 3D.

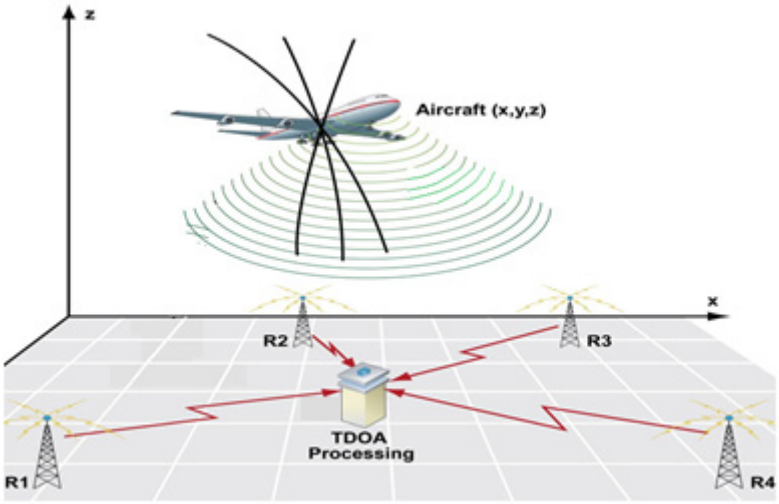


Figure 1: Four receivers multilateration configuration (Mike, 2009).

A link infrastructure is required in a multilateration system to connect all the receivers with the command centre to perform the necessary processing to locate the AE in real-time. The complexity and expanse of the link infrastructure influences the number and position of receivers, and the separation between receivers. For an instant, a larger separation between receivers improves PE by reducing the error but at the expense of a more extensive data link infrastructure. Multilateration systems for air traffic monitoring (ICAO, 2007) are normally located in build up areas with excellent data link infrastructure and can support a larger separation between receivers. However, mobile

deployment of multilateration systems for the military (Kopp, 2008) may require adhoc data link infrastructure which limits separation of receivers as well as the data transfer rates required for PE. Related works has suggested a range of receiver separation at a maximum of about 55 km (Neven *et al*., 2004) to a minimum separation of 9 km (Ujcova, 2013). A 10 km receiver separation is used in this paper to consider the possibility of deployment in an adhoc link structure. Further separation of receivers and antenna arrangement will be the subject of future investigation. This paper assumes the receiving antenna with a gain of 12 dBi with receiver sensitivity of -100 dBm (David, 2011). Due to the need to process the signal in digital technology, it is essential to decide on the appropriate choice of sampling frequency. A review of possible implementation technology based on radio frequency (RF) sensors (DTA, 2009; Keysight, 2015) and software defined radio (SDR) (Ettus Research, 2015) have shown that the technology is capable to perform sampling at frequencies above 40 MHz. With reference to the speed of light at 3×10^8 m/s, this sampling frequency allows resolving distances of 3×10^8 m/s x $1/(40 \times 10^6)$ s= 7.5 m.

Since the multilateration system's target application is to locate AE, it is necessary to have 360° PE coverage since the AE could approach in any direction and altitude. A square arrangement of receivers is the best due to its symmetry of arrangement. For example, a bearing of 45° has similar accuracy with the bearings of 135, 225 and 335°. By analysing a quadrant of the coverage, it is sufficient to assess the overall PE coverage for the complete system. Within a 90° quadrant, the bearing of 60° is similar to 30° except that the PE error between the two bearings is opposite in the *x*- and *y*-axis directions. Besides providing a 360° coverage, the symmetry of the square arrangement can be exploited to simplify the PE coverage of the system (Kirkwood, 2003).

2.2 Emitter Parameters

The two main sources of emissions used for surveillance by both the military and civil aviation are at 1,090 MHz and at 8 to 12 GHz (commonly referred as the X-band). Although lower frequency bands, such as the high frequency (HF), very high frequency (VHF) and ultra high frequency (UHF) bands are used for communications purposes, the signals in these bands are not considered since their traffic intensity is lower. The 1,090 MHz band is used by the transponder for ADS-B, SSR and IFF (ICAO, 2007; Francis *et al*., 2011)for emissions such as modes A, C and S for civil aviation, and modes 1 to 4 for the military. The aircraft weather radar operates in the X-band and the signaling method used is typically a simple pulse radar (Brad, 2003; Pierre, 2003). For the military, the X-band is also used for weapon control radars. The transmission power for the ADS-B, SSR and IFF signals varies with the aircraft category. A minimum transmission power of 125 W is specified for small aircrafts while for larger aircrafts, it is at 250 W (RTCA, 2009; Francis *et al*., 2011). For aircraft weather radars, the transmit power can be as low as 500 W but typically at 10 kW (Fred, 2010), which is also applicable for weapon control radars (Kopp, 2008). Since an aircraft is a mobile platform with limited space, an omnidirectional antenna with 3 dBi gain is normally used for the ADS-B, SSR and IFF transponders. However, antennas for weapon control and weather radars have a higher gain, typically at 35 dBi and narrow beam (less 3°) since the objective is respectively to locate cloud formations and other aircrafts, and also to search and track targets (Skolnik, 1990; ITU, 2003; Wolff, 2008).

2.3 Performance Measures

A set of performance measures is used to verify the PE coverage of the multilateration system. Since the system can be used for air traffic monitoring for civil aviation, the ICAO reduced vertical separation minimum (RVSM) (Doc 9574, 2001) as the maximum altitude error and FAA horizontal separation (FAA, 2014) are used as the benchmarks for the PE in altitude and horizontal separation respectively. RVSM is an initiative to optimise the air space by reducing the altitude separation between aircrafts from 600 m (2,000 ft) to 300 m (1,000 ft) for flight levels of 290 to 410 (29,000 to 41,000 ft). Based on the probability of height keeping error of less than 2×10^{-3}, the maximum altitude error based on a Gaussian probability density function (pdf) with three standard deviations is 30 m (Doc 9574, 2001). The horizontal separation used in this article is based on the definition by the FAA

at 9 km for selected air routes and conditions. Similarly, the assumption that Gaussian pdf is used with three standard deviations to determine the horizontal separation error works out to 1.5 km.

The PE error for a radar depends on whether it is a PSR, SSR or ADS-B. PSR estimates position based on the time difference between the transmit and return signals, while SSR and ADS-B provides position from the flight parameters broadcasted by the aircraft transponder. In general, the horizontal position comes from the global navigation satellite networks (GNSS) while the altitude is obtained from the onboard aircraft barometric altimeter. There are two types of PSR for detecting AE; air traffic monitoring and air defence. The PE error for PSR used in air traffic monitoring and air defence is summarised in Table 1. The azimuth error corresponding to the PE error in the horizontal plane increases with range since the radar beam spreads out over distance. Similarly, this is true for the altitude error for the air defence radar. The use of pulse compression signalling in air defence radar shown in Table 1 improves range resolution and the resulting range error. It can be seen that the altitude error of greater 0.2 km (200 m) for air defence radars does not meet the RVSM requirement for an altitude error of 30 m. However, both types of radars meet the FAA horizontal separation requirement with error of less than 1.5 km for ranges up to 360 km.

Table 1: Performance comparison between ATC (GMST, 2007) and air defence radars (Lockheed Martin, 2015).

Range (km)	ATC		Air Defence		
	Azimuth error (km)	Range error (km)	Azimuth error (km)	Range error (km)	Altitude error (km)
90	0.24	0.2	0.283	<0.05	0.274
180	0.48	0.2	0.566	<0.05	0.547
360	0.97	0.2	0.843	<0.05	1.09

As for SSR and ADS-B, the accuracy of less 0.37 km is ensured with 95% confidence at the PE in the horizontal plane, which means meeting the horizontal separation requirement (ICAO, 2007). With an altitude error of 30 m, the RVSM requirement is met. Thus, the best technology to meet the horizontal separation and RVSM requirements are SSR and ADS-B since both systems estimate separation independent of range. The only disadvantage is both systems require radio link from the aircraft to the receiver and therefore subjected to packet losses due to the propagation path loss (Strohmeier *et al*., 2014).

3. EMITTER POSITION ESTIMATION METHODOLOGY

The main objective of multilateration is to measure the time delay between each receiver and use the information to estimate the position of the AE. At each receiver, the signal is down converted from the radio frequency band to the intermediate frequency where the signal is sampled at the Nyquist rate to obtain its discrete time representation. Several methods can be used to estimate time delay (Yushi & Abdulla Waleed, 2005). In this paper, the cross correlation function is used because it is signal independent and it does not introduced artefacts that can obscure the true signal characteristics. For a given i^{th} and j^{th} receiver pair, the cross correlation function of the received signal is:

$$R_{ij}(m) = \frac{1}{N}\sum_{n=1}^{N-1} s_i(n)s_j^*(n-m) \tag{1}$$

where $x_i(n)$ and $x_j(n)$ are the signals in complex discrete-time representation, and N is the duration of the signal. The time-delay between the received signal pair estimated from the peak of the cross-correlation is:

$$m_{ij} = \arg\max_m \left(R_{ij}(m)\right) \qquad 0 \le m \le N-1 \tag{2}$$

The path difference obtained from the time-delay m_{ij} is:

$$\Delta d_{ij} = \frac{m_{ij} c}{f_s} \tag{3}$$

where c is the speed of light at 3×10^8 m/s and f_s is the sampling frequency at 40 MHz. For a multilateration system with an arbitrary number of receivers, the time-delay estimates are obtained based on the steps described from Eqs. 1 to 3.

Given the position of the AE in the Cartesian coordinate (x,y,z), the distance d_k to each of the k^{th} receiver can be calculated using the Euclidean distance:

$$d_k = \sqrt{(x\text{-}x_k)^2 + (y\text{-}y_k)^2 + (z\text{-}z_k)^2} \tag{4}$$

where (x_k,y_k,z_k) is the location of the k^{th} receiver. The path difference between each i^{th} and j^{th} receiver pair is:

$$\Delta d_{ij} = d_i - d_j \tag{5}$$

In the coordinate system, the altitude of the AE is defined in the z-axis, while the horizontal plane position is defined in the x- and y-axes. Equating the path difference estimated from the cross correlation function in Eq. 3 and the Euclidean distance in Eq. 5 forms the following relationship:

$$\frac{m_{ij} c}{f_s} = \sqrt{(x\text{-}x_i)^2 + (y\text{-}y_i)^2 + (z\text{-}z_i)^2} - \sqrt{(x\text{-}x_j)^2 + (y\text{-}y_j)^2 + (z\text{-}z_j)^2} \tag{6}$$

By generating a set equations for i=1 to 3, j=1 to 3 and $i\neq j$, the location of the AE in the (x,y,z) coordinates can be estimated by solving a set of 3 simultaneous equations with 3 unknowns.

All the possible path differences between the receiver pairs are defined as follows:

$$\begin{aligned} \Delta d_{12} &= d_1 - d_2 \\ \Delta d_{13} &= d_1 - d_3 \\ \Delta d_{32} &= d_3 - d_2 \\ \Delta d_{34} &= d_3 - d_4 \end{aligned} \tag{7}$$

By substituting Eq. 7 into Eq. 6, two plane equations are derived (Bucher & Misra, 2002) and the first equation is expressed as follows:

$$y = A_{123} x + B_{123} z + C_{123} \tag{8}$$

where the coefficients of the plane equation are:

$$\begin{aligned} A_{123} &= \left[\frac{\Delta d_{13} x_{21} - \Delta d_{12} x_{31}}{\Delta d_{12} y_{31} - \Delta d_{13} y_{21}} \right] \\ B_{123} &= \left[\frac{\Delta d_{13} z_{21} - \Delta d_{12} z_{31}}{\Delta d_{12} y_{31} - \Delta d_{13} y_{21}} \right] \\ C_{123} &= \left[\frac{\Delta d_{13} \left(\Delta d_{12}^2 + x_{12}^2 + y_{12}^2 + z_{12}^2 \right) - \Delta d_{12} \left(\Delta d_{13}^2 + x_{13}^2 + y_{13}^2 + z_{13}^2 \right)}{\Delta d_{12} y_{31} - \Delta d_{13} y_{21}} \right] \end{aligned} \tag{9}$$

The position difference pairs and position square difference pairs in Eq. 9 are defined as follows:

$$\begin{aligned} &x_{ij} = x_i - x_j, y_{ij} = y_i - y_j, z_{ij} = z_i - z_j \\ &x_{ij}^2 = x_i^2 - x_i^2, y_{ij}^2 = y_i^2 - y_i^2, z_{ij}^2 = z_i^2 - z_i^2 \\ &i = 1 \text{to} 4,\ j = 1 \text{to} 4, i \neq j \end{aligned} \tag{10}$$

The second plane equation is expressed as follows:

$$y = A_{234}x + B_{234}z + C_{234} \tag{11}$$

where the coefficients of the plane equation are:

$$\begin{aligned} A_{234} &= \left[\frac{\Delta d_{24} x_{32} - \Delta d_{23} x_{42}}{\Delta d_{23} y_{42} - \Delta d_{24} y_{42}} \right] \\ B_{234} &= \left[\frac{\Delta d_{24} z_{32} - \Delta d_{23} z_{42}}{\Delta d_{23} y_{42} - \Delta d_{24} y_{42}} \right] \\ C_{234} &= \left[\frac{\Delta d_{24} \left(\Delta d_{23}^2 + x_{23}^2 + y_{23}^2 + z_{23}^2 \right) - \Delta d_{23} \left(\Delta d_{24}^2 + x_{24}^2 + y_{24}^2 + z_{24}^2 \right)}{\Delta d_{23} y_{42} - \Delta d_{24} y_{32}} \right] \end{aligned} \tag{12}$$

Similar to the first plane equation, the position difference pairs and position square difference pairs are defined in Eq. 10.

From the plane equations in Eqs. 8 and 11, the next step is to estimate the z position and then use the results to estimate the position in the x- and y-axes. The first step is to equate the two equations to produce a linear equation that defines x as a function of z:

$$x = Dz + E \tag{13}$$

where the coefficients are:

$$\begin{aligned} D &= \left[\frac{B_{234} - B_{123}}{A_{123} - A_{234}} \right] \\ E &= \left[\frac{C_{123} - C_{234}}{A_{123} - A_{234}} \right] \end{aligned} \tag{14}$$

Substituting Eq. 13 back into Eq. 8 produces a linear equation for y as a function of z:

$$y = Fz + G \tag{15}$$

where the coefficients are:

$$\begin{aligned} F &= A_{123}D + B_{123} \\ G &= A_{123}E + C_{123} \end{aligned} \tag{16}$$

Eq. 15 is substituted back into Eq. 7 and further simplification is described in Bucher & Misra (2002), resulting in a quadratic equation in z. The solution z can be obtained by equating the function to zero:

$$Jz^2 - Kz + L = 0 \tag{17}$$

where the coefficients of the equations are:

$$
\begin{aligned}
J &= 4\Delta d_{13}^2\left[D^2 + F^2 + 1\right] \\
K &= 8\Delta d_{13}^2\left[D(x_1 - E) + F(y_1 - G) + z_1)\right] + 2IH \\
H &= \Delta d_{13}^2 + x_{13}^2 + y_{13}^2 + z_{13}^2 + 2x_{31}E + 2y_{31}G \\
I &= 2\left[x_{31}D + y_{31}F + 2z_{31}\right] \\
L &= 4\Delta d_{13}^2\left[(x_1 - E)^2 + (y_1 - E)^2 + z_1^2\right] - H^2
\end{aligned}
\tag{18}
$$

By applying the quadratic equation, the solution to z is:

$$
z = \frac{K}{2J} \pm \sqrt{\left(\frac{K}{2J}\right)^2 - \frac{L}{J}} \tag{19}
$$

With the solution to the altitude z, the horizontal locations x and y is obtained by substituting into Eqs. 13 and 15 respectively.

4. RESULTS AND DISCUSSION

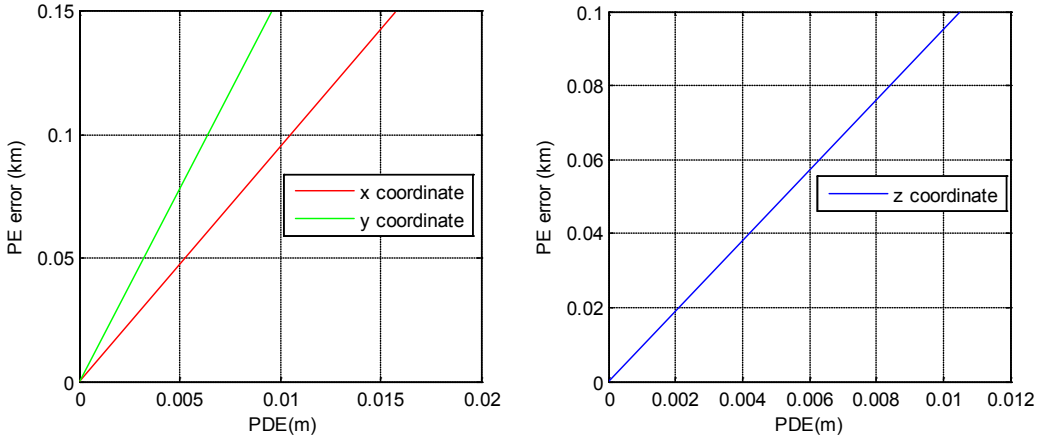
Monte Carlo simulations are conducted to first estimate the PE error due to the path difference estimation (PDE) and PE errors at various SNRs. The PE error is then benchmarked to the ICAO RVSM and FAA horizontal separation. Comparison of the PE error is also made with the relevant PSR. Finally, a procedure to verify the PE coverage of the multilateration system is described for various ranges, frequencies and transmitted powers of the emitter.

4.1 PE Error versus PDE Error

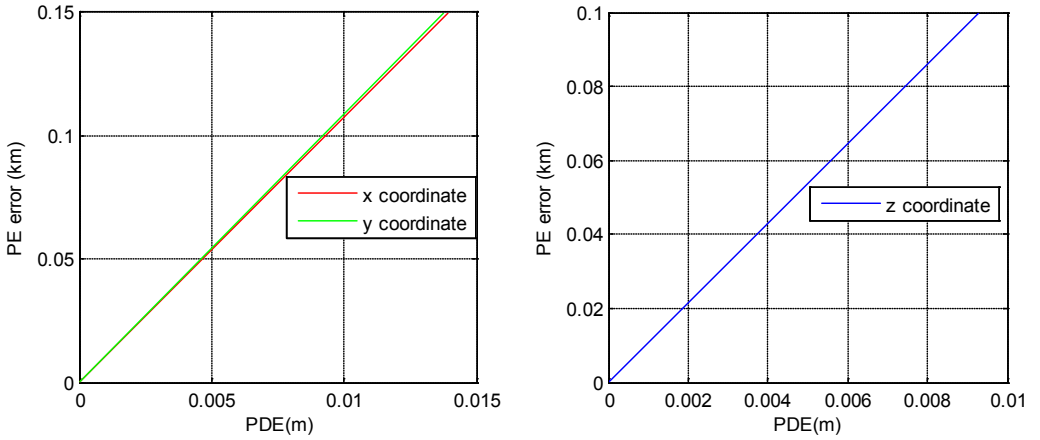
The complex nature of the relationship between the PDE and PE errors as described in Section 3 makes it difficult to establish a mathematical relationship between them. Thus, Monte Carlo simulations are used to establish this relationship.

By using a multilateration system with square receiver arrangement and separation of 10 km, a Gaussian random variable with zero mean and standard deviation is introduced in the j^{th} and k^{th} path difference in Eq. 7, and the PE is determined by using Eqs. 13, 15 and 19. The PDE error is included to consider the effect of quantisation error in analog to digital conversion, thermal noise in the received signal, signal attenuation due to path loss, and noise introduced by the receiver radio frequency front end. Monte Carlo simulations are conducted based on 100 trials for various standard deviations $\sigma_{v_{jk}}$ and selected AE positions relative to the multilateration system.

Figure 2 shows the PE and PDE errors for an AE located at altitude of 7 km, horizontal range of 20 km, and bearings of 45 and 60°. It is observed that the PE error increases linearly with the PDE error for a distance from 0 to 10 m. For the bearing of 60°, the PE error along the x-axis is lower compared to the y-axis. Due to the symmetry of the receiver arrangement, the opposite effect is true for the PE error on the x- and the y-axes for the bearing of 30°. The PE error is the same for the bearing of 45° on both the x- and the y-axes. Between the two bearings, 45° has slightly lower PE error on the z-axis.



(a)



(b)

Figure 2: PE error versus PDE error at bearings of (a) 45° and (b) 60° for altitude of 7 km and range of 20 km. The PE error for 30° is similar to 60° except that the PDE error in the *x*- and *y*-axes are reversed.

4.2 PE versus Range, Bearing and Altitude

All the possible PE errors are calculated for ranges of 20, 80 and 200 km; bearings of 30, 45 and 60°; and altitudes of 1, 7 and 15 km. By using the Monte Carlo simulation results in Section 4.1, Tables 2 and 3 are formed by using PDE errors of 2 and 4 meters respectively as a reference to determine if the multilateration system can resolve the AE position at a given range, bearing and altitude in conformance to the ICAO RVSM and FAA horizontal separation. In addition, performance comparison is made with the current technology used in the PSR for air defence radars previously described in Table 1.

The table entries that represent PE error are obtained for each AE location by considering the PE error in the horizontal plane and altitude error for a PDE error of 2 m. For example, from Table 2, for altitude of 7 km, bearing of 60° and horizontal range of 20 km, the PE errors in horizontal plane are 0.01876 and 0.03028 km respectively, while in altitude is 0.01876 km (18.76 m). Since the PE errors are within the RVSM (less than 30 m) and horizontal separation (less than 1.5 km) limits, the corresponding table entries are shaded in yellow and green for compliance to the benchmark for horizontal position and altitude respectively. An asterisk symbol * is marked to indicate if the PE error is lower compared to the air defence radar parameters described in Table 1. At a range of less than 20 km, the air defence radar range error is less than 0.05 km, which is better than the multilateration system. However, both the azimuth error at 0.283 km and altitude error at 0.274 km (274 m) are higher as compared to the multilateration system. The same procedure is applied for selected AE locations and the results are tabulated in Table 2. The PE error at PDE error of 4 m is presented in Table 3. Between Table 2 and Table 3, the PE errors are higher in Table 3. The

horizontal separation is complied for a maximum range less than 80 km, while both horizontal separation and attitude are complied for a maximum range less than 20 km at all altitudes. In comparison with the primary radar in Table 1, the multilateration system performs better at maximum range of less than 20 km and at a maximum altitude of 15 km. In general, the air defence radar meets the requirement for horizontal separation error, but does not meet the vertical separation error even at shorter ranges of less than 20 km.

Table 2: The PE error estimates at PDE error of 2 m. Yellow shade indicates compliance with the FAA horizontal separation, green shade indicates compliance with the ICAO RVSM and *indicates exceeding the air defence radar performance in Table 1.

Altitude (km)	Bearing (°)	Horizontal Range (km)	PDE error (m)	PE Error *x*-axis (km)	PE Error *y*-axis (km)	PE Error *z*-axis (km)
1	45	20	2	0.01796*	0.01796*	0.01833*
	30/60			0.01581*	0.02565*	0.01581*
	45	80		0.29710	0.29710	0.29710
	60			0.24060	0.41600	0.24060
7	45	20		0.02419*	0.02419*	0.02397*
	30/60			0.01876*	0.03028*	0.01876*
	45	80		0.29260	0.29260	0.29390
	30/60			0.25910	0.45030	0.25910
	45	200		2.03600	2.03600	2.03500
	30/60			1.59100	2.76300	1.59100
15	45	20		0.04020*	0.04020*	0.03991*
	30/60			0.03149*	0.05373*	0.03149*
	45	80		0.32760	0.32760	0.32560
	30/60			0.26310	0.45590	0.26310
	45	200		1.97400	1.97400	1.97300
	30/60			1.59500	2.77000	1.59500

Table 3: The PE error estimates at PDE error of 4 m. Yellow shade indicates compliance with the FAA horizontal separation, green shade indicates compliance with the ICAO RVSM and *indicates exceeding the air defence radar performance in Table 1.

Altitude (km)	Bearing (°)	Horizontal Range (km)	PDE error (m)	PE Error *x*-axis (km)	PE Error *y*-axis (km)	PE Error *z*-axis (km)
1	45	20	4	0.03887*	0.03625*	0.03887*
	30/60			0.03778*	0.06189*	0.03368*
	45	80		0.56250	0.56259	0.55950
	30/60			0.45450	0.79320	0.45460
7	45	20		0.04064*	0.04064*	0.04147*
	30/60			0.03630*	0.05699*	0.03630*
	45	80		0.56280	0.56280	0.57420
	30/60			0.52090	0.89770	0.52090
	45	200		3.02200	3.02200	3.03500
	30/60			2.91600	5.04300	2.91600
15	45	20		0.07480*	0.07480*	0.07817*
	30/60			0.058430*	0.09629*	0.05843*
	45	80		0.63180	0.63180	0.62840
	30/60			0.57470	0.88770	0.57470
	45	200		3.95300	3.95300	3.96300
	30/60			3.21700	5.59400	3.21700

4.3 TDE error versus SNR

The time delay between any two signals is estimated using the peak of the cross correlation function in Eqs. 1 and 2. Due to noise in the received signal, error is present in the TDE. This is significant since signals further away from the receiver have lower received power relative to the noise power as compared to the signals closer to the receiver. The noise power in relation to the signal power - defined by the SNR - affects the TDE error. By applying Eq. 3, the TDE error is translated to PDE error. Similar to PE error, the relationship between the TDE error with the SNR is established by using Monte Carlo simulations. Based on 100 trials for a given SNR, the relationship between the PDE error and SNR is shown in Figure 3. It is observed that PDE error decreases as SNR increases. At SNR greater than 24 dB, PDE error decreases linearly with SNR. By performing regression analysis for SNR from 24 dB to 34 dB, PDE errors of 4 m and 2 m are obtained at SNRs of 32 and 64 dB respectively. By cross referencing the PDE error with Tables 2 and 3, it is possible to determine the PE error for a given range and altitude. Further details on this procedure are described in the next subsection.

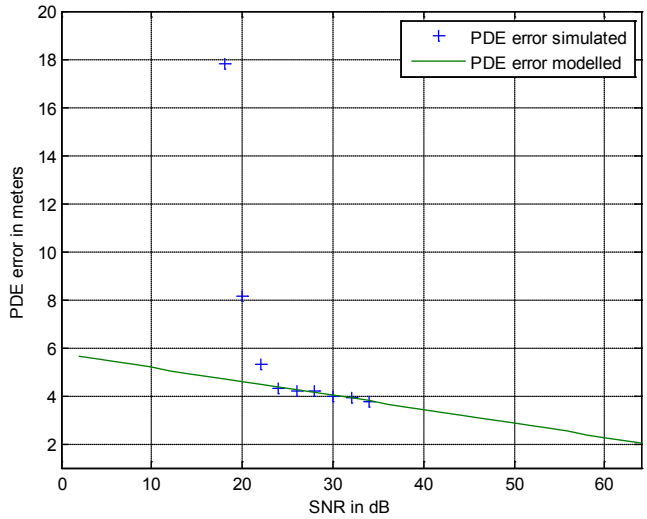


Figure 3: TDE error versus SNR.

4.4 PE Coverage of the Multilateration System

From the PE and PDE errors derived in Sections 4.2 and 4.3 respectively, the next step is to determine the PE coverage of the multilateration system with reference to the ICAO and FAA requirements, and in comparison to current air defence radars for a given operating frequency and transmit power. Based on PE and PDE errors, the PE coverage of the multilateration system can be verified by using the following procedure:

1. From the AE parameters described in Section 2.2, the received power at the ground station for a given location is calculated based on the free space loss formula (Ziemer & Peterson, 2001):

$$P_r = P_t + G_t + G_r - 32 - 20\log_{10} d_{km} - 20\log_{10} f_{MHz} \qquad (20)$$

   where P_t is the transmit power, G_t is the transmit antenna gain in dBi, G_r is the received antenna gain in dBi, d_{km} is the distance in km and f_{MHz} is the frequency in MHz.

2. The SNR is then estimated by taking the difference between the received power and receiver sensitivity.

3. From the estimated SNR, the PDE error is determined from Figure 3.

4. Depending on the PDE error, Table 2 is used for PDE error of 2 m to determine the PE error for locating an AE and determine if the error conforms to the benchmark and air defence radar technology. Similarly, Table 3 is used for PDE error of 4 m.

From the procedure described, an example is used to verify the PE coverage for an AE located at an altitude of 7 km with a range of 20 km from the system transmitting at a frequency of 1,090 MHz, transmit power of 250 W and antenna gain of 3 dBi. The parameters of the multilateration system are as described in Section 2.2, where the receiver sensitivity is -100 dBm and antenna gain is 12 dBi. Based on the free space loss propagation model, the received signal strength of -50 dBm is obtained and an SNR of 50 dB is obtained from the difference between the received signal strength and sensitivity. From Figure 4, the SNR of 50 dB gives a PDE error of 3 m. Thus, the estimated PE error should be between the results presented in Tables 2 and 3. At PDE error of 4 m, the average PE errors for the range of 20 m, bearing of 45° and altitude 7 m are about 0.04 km and 0.038 km (38 meters) for the horizontal plane and altitude respectively. The average PE errors for PDE error of 2 m are about 0.024 km and 0.02 km (20 meters) for the horizontal plane and altitude respectively. Due to the linearity in the PE error at SNR greater than 34 dB, as shown in Figure 4, the PE errors at PDE error of 3 m can be interpolated as 0.032 km and 0.029 km (29 meters) for the horizontal plane and altitude respectively. From these results, the PE coverage of the system with PE error in the horizontal plane of 0.32 m meets the FAA horizontal separation (error of 1.5 km) and is better than the azimuth error of 0.283 km for the air defence radar shown in Table 1. For the vertical axis, the multilateration system with the PE error in altitude of 0.029 km (29 meters) meets the ICAO RVSM requirement (vertical separation error of 30 m) and is better than the altitude error of 0.274 km (274 m) for the air defence radar.

The same procedure is then performed for the remaining selected AE positions, transmit powers and operating frequencies. The following sub-sections discuss the PE coverage for operating frequencies of 1,090 MHz and 10 GHz respectively based on the typical transmit power used by the AEs.

4.4.1 Operating Frequency of 1,090 MHz

The parameters of the transmitter and receiver for this example are as follows:

- Transmit power= 250 W
- Receiver sensitivity= -100 dBm
- Receiver antenna gain= 12 dBi
- Transmitter antenna gain= 3 dBi

Table 4 describes the PE coverages for the multilateration system at ranges from 20 to 200 km, at bearings from 30 to 60°, and received SNR from 25 to 50 dB. The PE coverage meets the ICAO RVSM for ranges of less than 20 km and the FAA horizontal separation for ranges less than 80 km. Compared to the air defence radar, the multilateration system's PE performance exceeds the radar for ranges less than 20 km.

4.4.2 Operating Frequency of 10 GHz

To verify the PE coverage in the 8 to 12 GHz band, the centre frequency at 10 GHz is selected. The parameters of the transmitter and receiver for this example are as follows:

- Transmit power= 500 and 5,000 W
- Receiver sensitivity= -100 dBm
- Receiver antenna gain= 12 dBi
- Transmitter antenna gain= 30 dBi

Table 4: PE coverage of the multilateration system at operating frequency of 1,090 MHz. Blue shade indicates PDE error between 2.5 to 4 m, yellow shade indicates compliance with FAA horizontal separation, green shade indicates compliance with ICAO RVSM, and * indicates exceeding the air defence radar performance in Table 1.

No.	Bearing (°)	Altitude (km)	Range (km)	Power Received (dBm)	SNR (dB)	PDE Error (m)	PE Error *x*-axis (km)	PE Error *y*-axis (km)	PE error *z*-axis (km)
1	30/45/60	1	20	-53	47	3.25	<0.03*	<0.03*	<0.03*
2			80	-63	37	3.6	<0.5	<0.5	<0.5
3		7	20	-53	47	3.25	<0.03*	<0.03*	<0.03*
4			80	-63	37	3.6	<0.5	<0.5	<0.5
5			200	-70	29	4.1	>3	>3	>3
8		15	20	-54	46	3.3	<0.03*	<0.03*	<0.03*
9			80	-63	37	3.6	<0.5	<0.5	<0.5
10			200	-70	29	4.1	>3	>3	>3

The PE coverages for the multilateration system at ranges from 20 to 200 km, bearings from 30 to 60° and received SNR from 40 to 68 dB are shown in Tables 5 and 6 for transmit powers of 500 and 5,000 W respectively. The multilateration system's PE coverage meets the ICAO RVSM for ranges of less than 20 km and FAA horizontal separation for ranges of less than 80 km for both the transmit powers. For transmit power of 500 W, the multilateration system's localisation performance exceeds the air defence radar for ranges of less than 20 km. The performance exceeds the air defence radar for ranges of up to 80 km if the transmit power is 5,000 Watts.

Table 5: PE coverage of the multilateration system at operating frequency of 10 GHz at transmit power of 500 W. Tan shade indicates PDE error of less than 2.5 m, blue shade indicates PE error between 2.5 to 4 m, yellow shade indicates compliance with FAA horizontal separation, green shade indicates compliance with ICAO RVSM, and * indicates exceeding the air defence radar performance in Table 1.

No.	Bearing (°)	Altitude (km)	Range (km)	Power Received (dBm)	SNR (dB)	PDE Error (m)	PE Error *x*-axis (km)	PE Error *y*-axis (km)	PE Error *z*-axis (km)
1	30/45/60	1	20	-42	58	2.4	<0.03*	<0.03*	<0.03*
2			80	-52	48	3.2	<0.5	<0.5	<0.5
3		7	20	-43	57	2.2	<0.03*	<0.03*	<0.03*
4			80	-52	48	3.2	<0.5	<0.5	<0.5
5			200	-60	40	3.5	>3	>3	>3
8		15	20	-43	57	2.2	<0.03*	<0.03*	<0.03*
9			80	-52	46	3.3	<0.5	<0.5	<0.5
10			200	-60	40	3.5	>3	>3	>3

Table 6: PE coverage of the multilateration system at operating frequency of 10 GHz at transmit power of 5,000 W. Tan shades indicare PDE error of less than 2.5 m, blue shade indicates PE error between 2.5 and 4 m, yellow shade indicates compliance with FAA horizontal separation, green shade indicates compliance with ICAO RVSM, and * indicates exceeding the air defence radar performance in Table 1.

No.	Bearing (°)	Altitude (km)	Range (km)	Power Received (dBm)	SNR (dB)	PDE Error (m)	PE Error *x*-axis (km)	PE Error *y*-axis (km)	PE Error *z*-axis (km)
1	45/60	1	20	-32	68	1.8	<0.02*	<0.02*	<0.02*
2			80	-42	58	2.4	<0.30*	<0.30*	>0.300*
3		7	20	-32	68	1.8	<0.02*	<0.02*	<0.02*
4			80	-42	58	2.4	<0.30*	<0.30*	>0.300*
5			200	-50	50	2.9	>1.500	>1.500	>1.500
8		15	20	-32	68	1.8	<0.03*	<0.03*	<0.03*
9			80	-42	58	2.4	<0.300*	<0.300*	>0.300*
10			200	-50	50	2.9	>1.500	>1.500	>1.500

4.5 Discussion

The analysis of PE coverage shows that the multilateration system can provide accurate position in 3D at range of less than 20 km, meeting the FAA horizontal separation and ICAO RVSM requirements as well as exceeding the performance of the air defence radar. Between 20 to 80 km, all the requirements are met except for the ICAO RVSM, as shown in Subsection 4.4.2 for operating frequency of 10 GHz at transmit power of 5,000 Watts. This is a realistic assumption since the transmit power for fighter and strike aircrafts are typically above 5,000 W (Kopp, 2008). The PE coverage could be further extended for ranges of up to 200 km if the AE is an airborne early warning aircraft, where the peak transmit power could go as high as 1 MW (Surveillance, 2015). It is also important to note that multilateration systems are identified as an anti-stealth technology (Saxena, 2012), which makes it an important component for future air defence infrastructure to complement with the current primary and secondary radar systems. From the economics perspective, a multilateration system for a given PE coverage is still cheaper in terms of the equipment acquisition and maintenance compared to a PSR (ICAO, 2007; Rechy-Ramirez & Hu, 2011; Multilateration & ADS-B, 2015).

This paper considers a minimum configuration system with four receivers which enables for position estimation of AE in 3D. The separation of receivers is limited to 10 km to consider deployment where there is limited communication infrastructure and to facilitate its deployment to support mobile units. If line of sight data link is used, the curvature of the earth and terrain limits the separation of receivers. The separation of receivers can be increased in the multilateration system to improve the PE coverage if the existing communications infrastructure can be used to provide the data link between the components of the multilateration system. With larger receiver separation, the expected lower PDE error results in lower PE error. As an extension of this work, a methodology should be developed to determine the PE coverage for an arbitrary multilateration system structure without using Monte Carlo simulations as done with the present approach. Once the structure and the coverage area is decided, Monte Carlo simulations should only be used sparingly to verification purposes.

5. CONCLUSION

Multilateration is a surveillance system that complements existing technologies such as PSR, SSR and ADS-B. It employs TDOA estimation to estimate the position of the AE. This paper describes the methodology for implementing and verifying a minimum configuration of four receivers multilateration system. The benchmark used to verify the system's PE coverage performance is based on the ICAO RVSM, FAA horizontal separation and current air defence radar technology. Based on the methodology, the PE coverage for the system benchmarked to the relevant standards and current

air defence radar is up to 20 km in 3D and up to 80 km in 2D. If compliance to standards is not critical and the main objective is to detect AEs, the system is able to cover up to 200 km in 2D with PE error of 1.5 km.

ACKNOWLEDGEMENTS

The authors would like to thank Universiti Teknologi Malaysia (UTM) under project Vot No. Q.J130000.3023.00M13 and Ministry of Higher Education (MOHE) Malaysia for providing the resources for this research.

REFERENCES

Brad, P. (2003). Troubleshooting airborne weather radar. *Avionics News*, **November 2003**: 52–55.

Bucher, R., & Misra, D. (2002). A synthesizable VHDL model of the exact solution for three-dimensional hyperbolic positioning system. *VLSI Des.*, **15**: 507–520.

David, W. (2011). Airborne Weather Radar. *Avionics News*, **April 2011**: 74–81.

Dhull, S., & Sahu, O. P. (2010). Comparison of time-delay estimation techniques in acoustic environment. *Int. J. Comput. Appl.*, **8**: 29–31.

DTA. (2009). Sensor Signal Acquisition , Recording & Playback for Demanding Applications. D-TA System Inc. Retrieved from www.d-ta.com (Last access date: 10 January 2015).

Ettus Research. (2015). *USRP N210.* Available online at: http://www.ettus.com/product/category/USRP-Networked-Series (Last access date: 11 January 2015).

Falk, J. (2004). *An Electronic Warfare Perspective on Time Difference of Arrival Estimation Subject to Radio Receiver Imperfections*. Royal Institute of Technology, Stockholm, Sweden.

FAA (Federal Aviation Administration) (2014). *Air Traffic Control*. Federal Aviation Administration (FAA), US Departement of Transportation, Washington D.C.

Francis, R. (2011). *Handbook: Spectrum Monitoring, 2nd Ed*. International Telecommunication Union (ITU), Geneva.

Francis, R., Vincent, R., Noël, J. M., Tremblay, P., Desjardins, D., Cushley, A. & Wallace, M. (2011). The flying laboratory for the observation of ADS-B signals. *Int. J. Nav. Observation*, **Vol. 2011**: Article ID 973656.

Fred, P. R. (2010). *Airborne Weather Radar - Separating Fact from Fiction*. Available online at: http://www.helicoptermaintenancemagazine.com/article/airborne-weather-radar-separating-fact-fiction (Last access date: 15 January 2015).

Gustafsson, F. & Gunnarsson, F. (2003). Positioning using time-difference of arrival measurements. *2003 IEEE Int. Conf. Acoustics, Speech Signal Proc. (ICASSP '03),* Vol. 1, pp. VI–553–6.

ICAO (International Civil Aviation Organization) (2001). *Doc 9574: Manual on Implementation of a 300 m (1 000 ft) Vertical Separation Minimum Between FL 290 and FL 410 Inclusive*. International Civil Aviation Organization (ICAO), Montreal, Quebec.

ICAO (International Civil Aviation Organization) (2001). *Guidance Material on Comparison of Surveillance Technologies (GMST)*. International Civil Aviation Organization (ICAO), Montreal, Quebec.

ITU (International Telecommunication Union) (ITU). (2003). *M.1464: Characteristics of Radiolocation Radars, and Characteristics and Protection Criteria for Sharing Studies for Aeronautical Radionavigation and Meteorological Radars in the Radiodetermination Service Operating in the Frequency Band 2,700-2,900 MHz*. International Telecommunication Union) (ITU)

Keysight (2015). N6841A RF Sensor. *Keysight Technology*. Available online at: http://www.keysight.com/en/pd-1414739-pn-N6841A/rf-sensor?cc=MY&lc=eng (Last access date: 15 January 2015).

Kirkwood, B. (2003). *Acoustic Source Localization Using Time-Delay Estimation*. M.Sc. Thesis, Technical University of Denmark, Kongens Lyngby, Denmark.

Kopp, C. (2008). *Assessing Russian Fighter Technology.* Available online at: http://www.ausairpower.net/APA-2008-04.html (Last access date: 15 January 2015).

Lockheed Martin. (2015). *Ground-Based Air Surveillance Radars*. Available online at: http://www.lockheedmartin.com/us/products/ground-based-air-surveillance.html (Last access date: 17 January 2009).

Mahdinejad, K., & Seghaleh, M. Z. (2013). Implementation of time delay estimation using different weighted generalized cross correlation in room acoustic environments. *Life Sci. J.*: **10**: 846–851.

Mike, M. (2009). *New Radar Sensors Improve Colorado Air Traffic Safety*. Available online at: http://avstop.com/news2/wide_area_multilateration_colorado.htm (Last access date: 17 January 2015).

Multilateration & ADS-B. (2015). *Multilateration & ADS-B: Executive Reference Guide*. Available online at: http://www.multilateration.com/downloads/1/1/210.html (Last access date: 11 January 2015).

Neven, W. H. L., Quilter, T. J., Weedon, R. & Hegondoorn, R. A. (2004). *Wide Area Multilateration Report on EATMP TRS 131/04*. National Aerospace Laboratory (NLR), Amsterdam.

Pierre, P. (2003). *Technical Notes: RADAR Spectral Bands*. Integrated Communication Technologies (ICT), Arlington, Virginia

RCTA (Radio Technical Commission for Aeronautics) (2009). *DO-260A: Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B)*. Radio Technical Commission for Aeronautics (RTCA), Washington D.C.

Rechy-Ramirez, E. J., & Hu, H. (2011). *Stages for Developing Control Systems Using EMG and EEG Signals : A Survey*. Technical Report CES-513, University of Essex, Colchester, Essex.

Rohde & Schwarz. (2008). *Radiomonitoring and Radiolocation*. Rohde & Schwarz GmbH, Munich

Saxena, V. K. (2012). Stealth and counter-stealth some emerging thoughts and continuing debates. *J. Defence Stud. Publ. Details*, **6**: 19–28.

Skolnik, M.I. (1990). An introduction to radar. *In* Skolnik, M.I. (Ed.), *Radar Handbook,* 2nd Ed., McGraw-Hill, New York, pp 1.11-1.18

Strohmeier, M., Schäfer, M., Lenders, V. & Martinovic, I. (2014). Realities and challenges of nextgen air traffic management: The case of ADS-B. *IEEE Commun. Mag.*, **52**: 111–118.

Surveillance, S. (2015). Awacs Surveillance Radar: The Eyes of the Eagle. Northrop Grumman : Electronic Systems. Avilable online at: www.northropgrumman.com/capabilities/awacsapy2/documents/awacs.pdf (Last access date: 17 January 2015).

Ujcova, M. (2013). Intelligent multiration system for air transport. *Eur. Int. J. Sci. Tech.,* **2**: 69–74.

Wiley, G. R. (2006). *ELINT: The Interception and Analysis of Radar Signals*. Artech House , London.

Wolff, C. (2008). *Air-Defense Radars*. Available online at: http://www.radartutorial.eu/02.basics/Air-Defense Radars.en.html (Last access date: 17 January 2015).

Zhang, X.F. & Xu, D.Z. (2009). Novel joint time delay and frequency estimation method. *IET Radar Sonar Nav.*, 3: 186-194.

Yushi, Z., & Abdulla Waleed, H. (2005). *A Comparative Study of Time-Delay Estimation Techniques Using Microphone Arrays*. School of Engineering Report No. 619, Faculty of Engineering, The University of Auckland, Auckland.

Zhang, L., Deng, K., Wang, H. & Luo, M. (2013). Time-delay estimation of multiple targets with wavelet based phase-only matched filter. *Int. J. Electron.*, **101**: 963–975.

Ziemer, R. E., & Peterson, R. L. (2001). *Introduction to Digital Communication*. Prentice-Hall International, Upper Saddle River, New Jersey.

DEVELOPMENT OF A PULSE REPETITION INTERVAL (PRI) MODULATION TEMPLATE USING WALSH- HADAMARD TRANSFORM (WHT)

Kamaruddin Abdul Ghani[1*], Kaharudin Dimyati[1] & Ahmad Zuri Sha'ameri[2]

[1]Department of Electrical & Electronic Engineering, National Defence University of Malaysia (NDUM), Malaysia
[2]Faculty of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Malaysia

*Email: kamaruddin@upnm.edu.my

ABSTRACT

The classification of pulse repetition interval (PRI) modulation types using transformation techniques has some disadvantages, whereby PRIs can be misclassified. In this study, classification of PRI modulation types is done using the power spectrum of the Walsh-Hadamard transform (WHT). The generated spectrums are downsampled to reduce sampling errors and sub-harmonics, resulting in decimated Walsh-Hadamard transform (DWHT) spectrums. A template of DWHT spectrums is developed for the most common PRI modulation types, which are; constant, jittered and staggered. In this template, each pulse sequence is given a unique DWHT spectrum as its identity. The template can be used as rule-based classifier for accurate identification of signals.

Keywords: *pulse repetition interval (PRI) modulation; Walsh-Hadamard transform (WHT); decimation rate; power spectrum.*

1. INTRODUCTION

The objective of Electronic Intelligence (ELINT) is to analyse pulse trains of radar signals and derive information from it. This is done by signal sorting to separate each pulse burst from signal flows of a large number of random overlapping pulses, and then selecting the useful deinterleaved signals (Jiang, *et al*., 2013). The deinterleaving process is often carried out via clustering of multiple inter pulse parameters such as time of arrival (TOA), pulse width (PW), angle of arrival (AOA), and radio frequency (RF) (Mahmoud *et al*.,2012). The measured parameters of every pulse are encoded in a digital format known as pulse descriptor words (PDW) (Li *et al*., 2013). The information is then extracted from it to identify the pulse repetition intervals (PRIs) so as to estimate PRI modulation types. Every radar signal has a unique signature that can be used to identify the PRI modulation type. The most common PRI modulation types are constant, jittered and staggered (Jingyao *et al*., 2009).

Most of the works on radar signal deinterleaving methods are based on statistical techniques and histograms (Mardia, 1989; Milojevic & Popovic, 1992; Guohua *et al*., 2009) and among the problems faced were inability to distinguish between radars signals having close PRIs and issues with subharmonics. Recent works have reported on the use of transformation techniques for PRI modulation identification to address these problems. Nishiguchi (2005) demonstrated that through PRI transformations, it is possible to obtain a power spectrum from which we can estimate the number of signal sources and their PRIs. Yan *et al*., (2009) and Mahdavi & Pezeshk (2011) have enhanced PRI transformations where they focused on suppressing PRI sub-harmonics while some of the works have focused on the robustness of the system against the effects of missing and spurious pulses (Jingyao *et al*., 2009; Guobing & Yu, 2010). However, these transforms have some drawbacks, where

they fit for constant and jittered PRIs, but not for staggered PRIs (Yan *et al*., 2009), in addition to poor handling capacity for jittered PRIs (Peizhi *et al*., 2012).

In this work, a methodology using Walsh-Hadamard transform (WHT) is developed to classify PRI modulations based on the power spectrum of pulse trains. A template of WHT spectrums is developed for constant, jittered and staggered intervals. Unique identities are allocated for the intervals so that appropriate classification can be made even for pulse trains having short PRIs.

2. WALSH-HADAMARD TRANSFORM (WHT)

In time series analysis, transform methods can be a prominent tool. WHT, which deals with the non-sinusoidal orthogonal transforms, has gained prominence in various digital signal processing applications as it can essentially be computed using only additions and subtractions (Ahmed & Rao, 1975; Yusuf *et al*., 2011).

The complete set of Walsh functions, which form complete orthogonal sequences on the unit interval [0,1] can be divided into two groups of even and odd functions about the point $t = 0.5$. These even and odd functions are analogous to the sine and cosine functions respectively. Hence they are denoted by sal (*s*ine W*al*sh) and cal (*c*osine W*al*sh) respectively, while Walsh is denoted by wal (Ahmed & Rao, 1975). By analogy, the power spectrum of a WHT is defined as the sum of the squares of the cal and sal coefficients. Walsh representation of signals is analogous to the Fourier (trigonometric) representation except that square waves are used as the basis function unlike complex exponentials used in Fourier transform (Ahmed & Rao, 1975). Figure 1 shows the strong resemblance between Fourier sinusoids and Walsh functions.

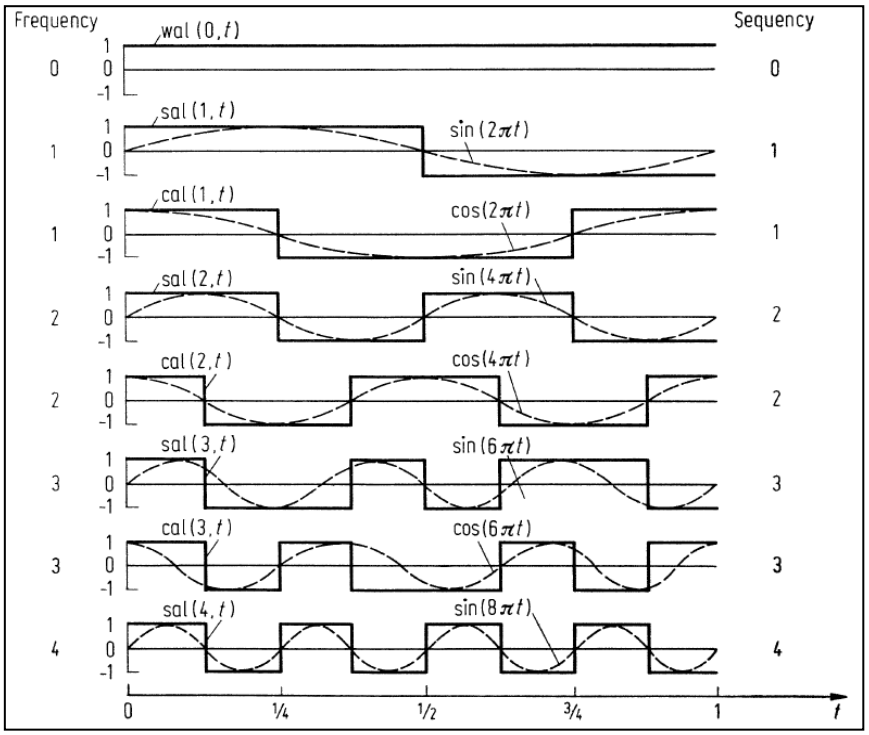


Figure 1: The resemblance between Fourier sinusoids and Walsh functions (Ahmed & Rao, 1975).

WHT is used for the Walsh representation of the data sequences. WHT decomposes the signal *x(t)* from its original domain to the set of the rectangular functions from the orthogonal basis (Maertins, 1999). Their basis functions are sampled Walsh functions that can be expressed in terms of symmetric matrices known as the Walsh-ordered Hadamard matrices $\mathbf{H}_h(n)$ where the subscript h denotes Hadamard ordering. In general, an (N x N) matrix $\mathbf{H}_h(n)$ would be obtained, where $n = \log_2 N$. This class of Hadamard matrices can be partitioned in the form:

$$\mathbf{H}_h(n)=\begin{bmatrix}\mathbf{H}_h(n-1) & \mathbf{H}_h(n-1)\\ \mathbf{H}_h(n-1) & -\mathbf{H}_h(n-1)\end{bmatrix} \quad (1)$$

and, are considered to be in natural form i.e. natural ordering (Ahmed & Rao, 1975). Assume that the radar pulse train is represented by the function $x(t_i)$, which indicates the time of arrival (TOA) of the i^{th} pulse. The transformation of Walsh-Hadamard spectrum $X(f)$ is indicated as:

$$X(f) = \int x(t_i)\, b(t,f)\, dt \quad (2)$$

where, $b(t,f)$ represents the square wave, and t and f are the time and frequency respectively.

The matrix $\mathbf{H}_h(n)$ contains numbers equal to -1 or 1, and can be determined from a simple recurrent expression (Ahmed & Rao, 1975):

$$\mathbf{H}_h(k)=\begin{bmatrix}\mathbf{H}_h(k-1) & \mathbf{H}_h(k-1)\\ \mathbf{H}_h(k-1) & -\mathbf{H}_h(k-1)\end{bmatrix}, k=1,2,3...n \quad (3)$$

where, $\mathbf{H}_h = [1]$, is the initial matrix. For example, the Hadamard matrices with order $k = 4$ obtained from Eq. 3 yields

$$\mathbf{H}_4 = \begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} \quad (4)$$

Walsh functions are rectangular or square waveforms that take only two values, +1 or -1 (or 'on' and 'off'). However, in this work, -1 is represented by '0' to simulate radar signal pulse train. The value of the function is logic value "0" or "1", which indicates no presence pulse and the presence of pulse respectively. Thus, the WHT will introduce a non-zero term at $X(0)$, indicating the presence of a direct current (DC) off set in the input pulse train.

3. METHODOLOGY

The PRI modulation type is determined by the interval between pulses. In this work, sequences of pulse train signals are simulated based on the most common PRI modulation types, which are constant, jittered and staggered, as shown in Figure 2. Constant PRI means the interval between every two adjacent pulses is a constant; jittered PRI means the interval is about a mean value but with a random jitter (maximum of ± 30%); while staggered PRI means the interval is a repetition of several fixed values (Jingyao, 2009). Staggered intervals can be further be broken down into more specific

groups depending on the level of staggered which is the number of different intervals before the repetition of the pattern (Abel, 1995).

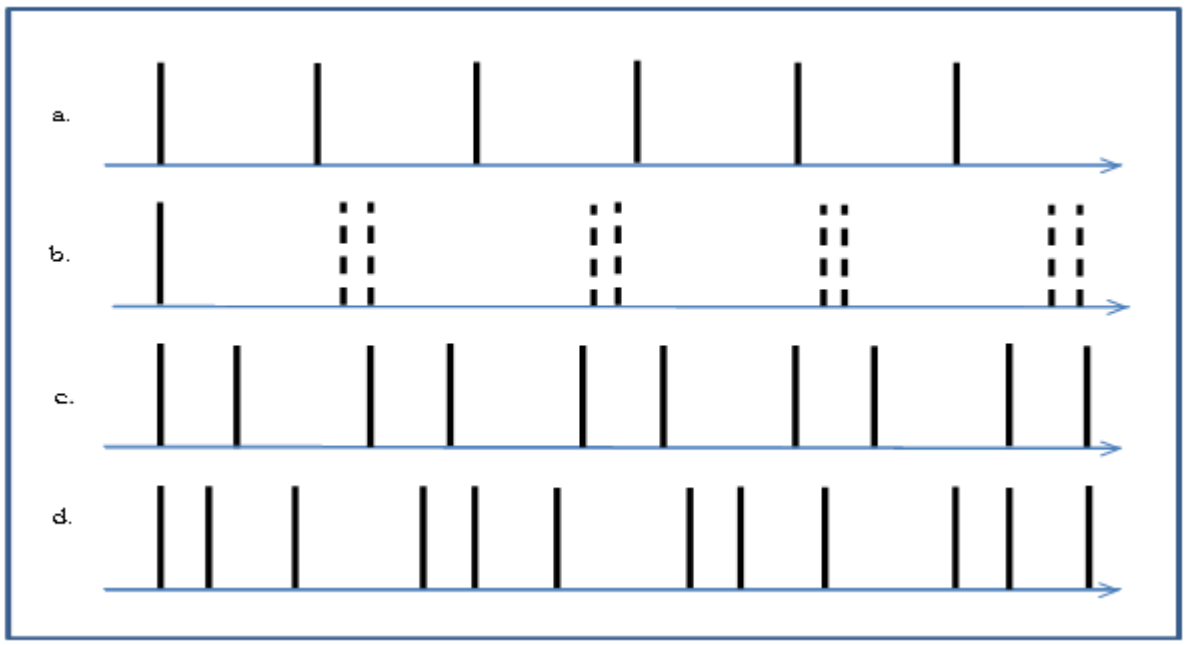


Figure 2: PRI representation of pulse trains for (a) constant (b) jittered (c) 2-level staggered (d) 3-level staggered.

Figure 3 shows the flowchart of the algorithm for classification of PRI modulations based on the power spectrum of pulse trains using WHT. Mathematical modelling of the sequences of pulse trains is developed to simulate the intercepted pulse train radar signals. The development of the PRI modulation template is focused on the most common intervals, including constant PRI with the shortest interval and level of staggered intervals. The PRI modulations are transformed using WHT for their power spectrum at 16^{th} order or higher to get a unique spectrum for every sequence of the pulse train signals.

Typically radar systems employ high enough sampling rate of analog-to-digital (A/D) converters to ensure that the number of samples required is sufficient for the processing. It is often the case that some radar signals are sampled at much higher rate than actually needed (Mahafza, 2009), which results in multiple peaks and subharmonics of spectrums. These errors can cause problems in distinguishing between radar signals having close PRIs (Nishiguchi, 2000). Therefore, the decimation of samples is needed to reduce these errors. The sampling rate is decreased by increasing the time steps between successive samples. If t_1 and t_2 are the original and decimated sampling intervals respectively, then

$$t_2 = Dt_1 \tag{5}$$

where D is the decimation ratio. The WHT spectrum is decimated to achieve the minimum number of peaks, resulting in a decimated WHT (DWHT) spectrum. The rate is limited to 4 due to the sequence length.

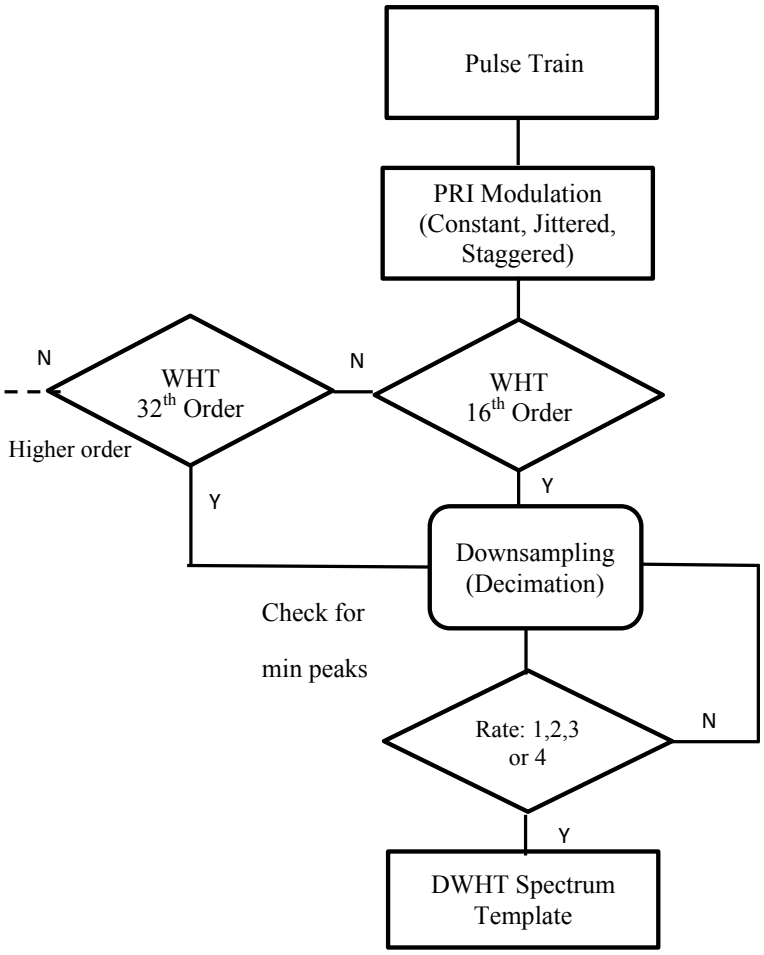


Figure 3: Flow chart classification of PRI modulation types using WHT.

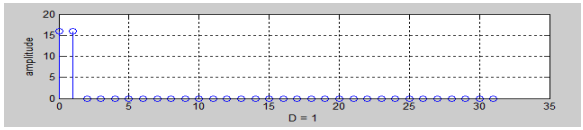
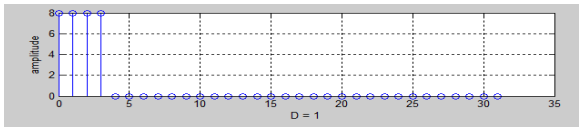
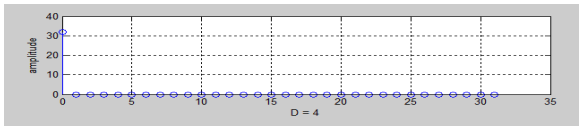
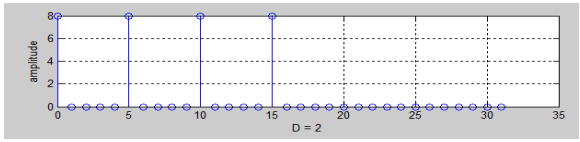
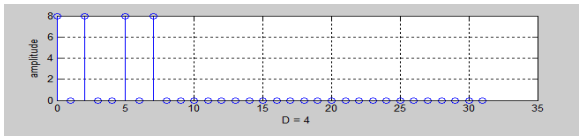
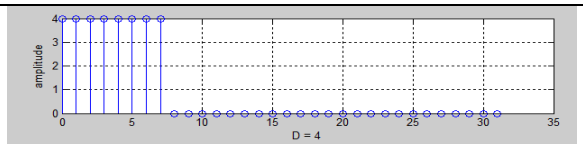
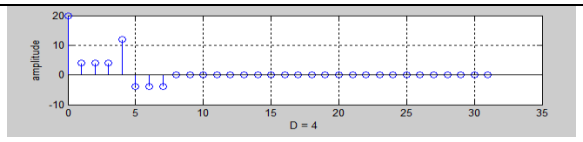
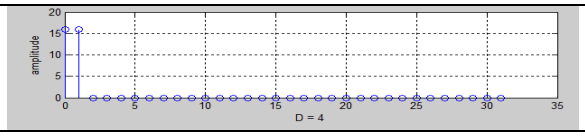
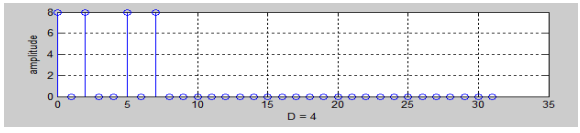
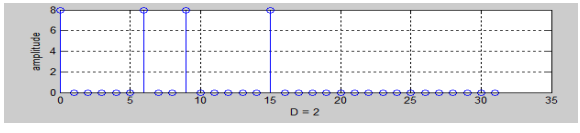
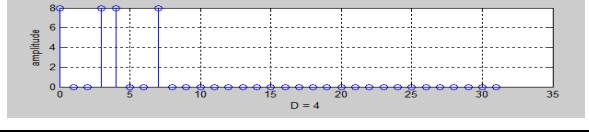
4. RESULTS AND DISCUSSION

Eight sequences of pulse trains are considered for this work, as tabulated in Table 1. Sequences 1 to 3 represent constant intervals with short, intermediate and long intervals respectively. Sequences 4 and 5 represent trains with jittering qualities with maximum jitter of up to 20 and 30% respectively. Three types of staggered pulse trains are simulated and they are represented by sequences 6 to 8.

The power spectrums for the sequences at the relevant decimation rates are obtained with some sequences having more than one possible spectrum, such as sequences 2, 3 and 8. With the 16^{th} order WHT, not all of the sequences show good spectrum, thus the transforms are carried out at the 32^{th} order.

Figure 4 shows the downsampling of the WHT spectrum for a 3-level staggered pulse sequence. A good power spectrum with minimum number of peaks was achieved at rate of $D = 4$, whereby other decimation rates cause a number of multiple peaks (positive and negative), as shown in Figure 5.

Table 1: Pulse train sequences and their WHT spectrums.

Sequence No	PRI Types	WHT Spectrum
1	Constant (short interval)	
2	Constant (intermediate interval)	 
3	Constant (long interval)	 
4	Jittered 20%	
5	Jittered 30%	
6	2-level Staggered	
7	3-level Staggered	
8	4-level Staggered	 

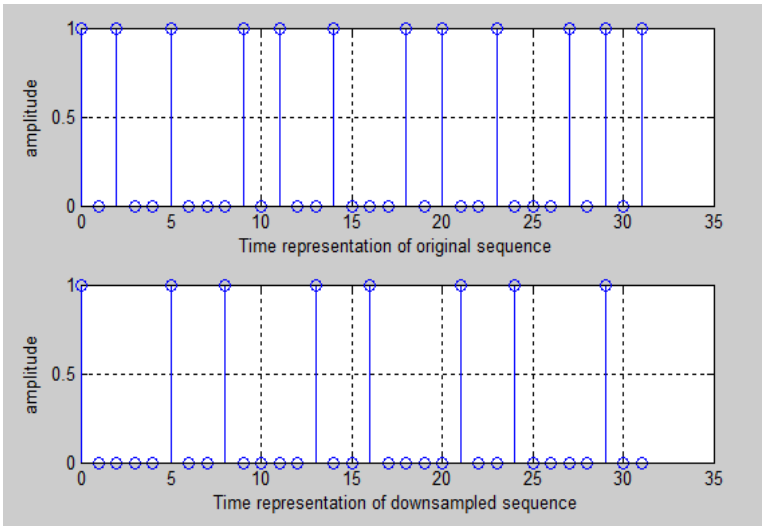


Figure 4: Downsampling of a 3-level staggered pulse sequence.

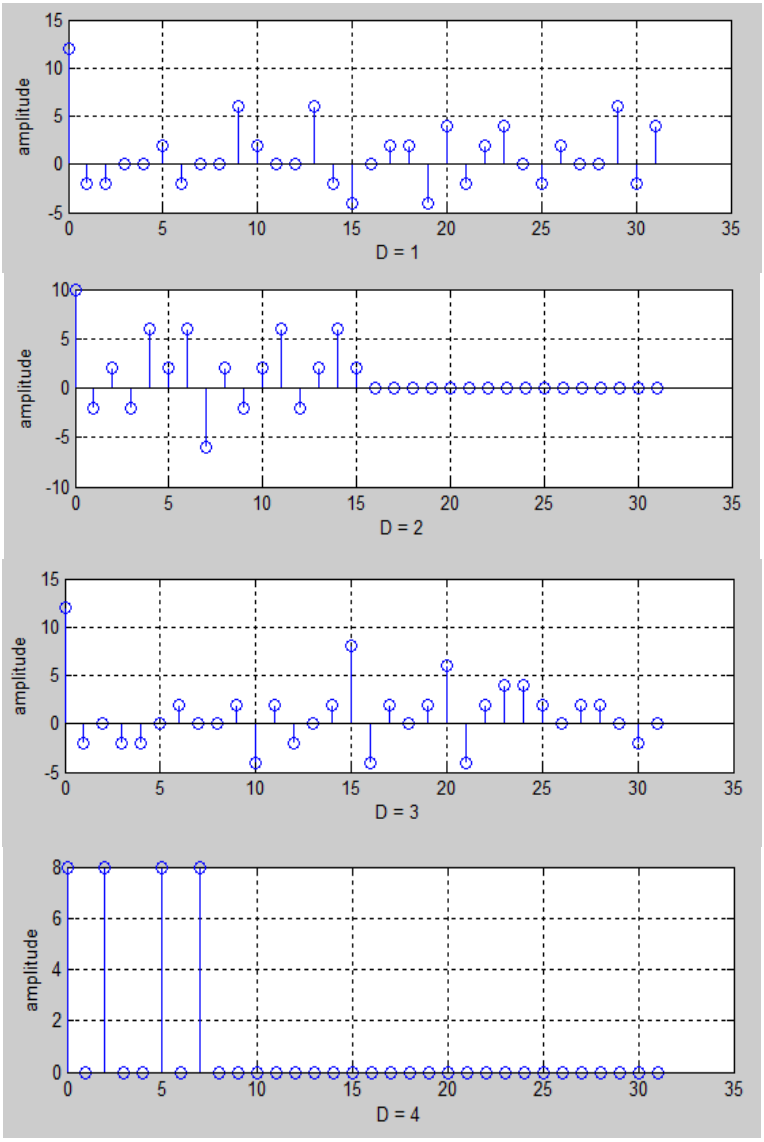


Figure 5: DWHT spectrums for the 3-level staggered pulse sequence in Figure 4 at D =1, 2, 3 and 4.

For the template, there is a need for each power spectrum to be unique, so only one spectrum is chosen for each sequence. The idea is for each PRI modulation type to have a specific power spectrum as its identity. Table 2 shows the selected DWHT template for the sequences. The problem of distinguishing radar signals having close PRIs can be solved since the constant short interval type has a dedicated DHWT spectrum that is different from constant intermediate and long interval types. Jittered PRI can also be distinguished, whereby the 20% jittered type has a rather good spectrum. However, for the 30% jittered type, the DWHT spectrum is somewhat random and needs further attention. The DWHT template not only can distinguish staggered pulse sequences from constant or jittered types, but can also differentiate among the levels of stagger, i.e., levels 2, 3 or 4.

Table 2: Template of DWHT spectrums for the pulse sequences.

PRI Modulation Type	Decimation Rate	DWHT
Constant (short interval)	1	$X(0)=16$, $X(1)=16$
Constant (intermediate interval)	4	$X(0)=32$
Constant (long interval)	2	$X(0)=8$, $X(5)=8$, $X(10)=8$, $X(15)=8$
Jittered (20%)	4	$X(0)=4$, $X(1)=4$, $X(2)=4$, $X(3)=4$, $X(4)=4$, $X(5)=4$, $X(6)=4$, $X(7)=4$
Jittered (30%)	4	$X(0)=20$, $X(1)=4$, $X(2)=4$, $X(3)=4$, $X(4)=12$
2-level Staggered	4	$X(0)=16$, $X(1)=16$
3-level Staggered	4	$X(0)=8$, $X(2)=8$, $X(5)=8$, $X(7)=8$
4-level Staggered	4	$X(0)=8$, $X(3)=8$, $X(4)=8$, $X(7)=8$

5. CONCLUSION

In this study, a template for classification of constant, jittered and staggered PRI modulation types was developed based on power spectrums of DWHT. The DWHT spectrums are unique for each PRI modulation type, and can be used to distinguish for signals having close PRIs and various levels of staggered signals. The template represents the PRI modulation which can be used to classify PRI types of pulse train signals. Identification of emitters can then be determined through matching procedures with database or threat libraries. Verification procedures for accuracies and robustness may need to be undertaken whereby future works may include the effects of missing and spurious pulses.

ACKNOWLEDGEMENT

This research work is supported by the FRGS Grant (FRGS/2/2014/TK03/UPNM/02/3).

REFERENCES

Abel, J. (1995). *SARIE: Groundbased Semi-Mobile ELINT*. Training Manual, Sysdel bk, Pretoria, South Africa.

Ahmed, N. & Rao, K.R. (1975). *Orthogonal Transforms for Digital Signal Processing*, Springer-Verlag, New York.

Guobing, H. & Yu, L. (2010). An efficient method of pulse repetition interval modulation recognition. *Int. Conf. Comm. and Mobile Comput.*, 287-291.

Guohua, G., Yan, M., Jun, H. & Xu, Q. (2009). An improved algorithm of PRI transform. *Global Congress Int. Sys.*, pp. 145-149.

Jiang, Y., Haiqing, J. & Zhenxing, L. (2013). Design and implementation on sorting and tracking processor for radar rignal based on DSP. *World Congress Soft. Eng*., pp. 145-149.

Jingyao, L., Huadong, M. & Xiqin, W. (2009). A new pulse deinterleaving algorithm based on multiple hypothesis tracking, *Int. Radar Conf.*, pp. 1-4.

Li, C., Wang, W. & Wang, X. (2013). A method of extracting radar words of multi-function radar at data level. *IET Int. Radar Conf*., pp. 1-5.

Maertins, A. (1999). *Signal Analysis: Wavelets, Filter Banks, Time-Frequency Transforms and Applications*. John Wiley & Sons, New York.

Mahafza, B. (2009). *Radar Signal Analysis and Processing Using MATLAB*. Chapman & Hall, Boca Raton.

Mahdavi, A. & Pezeshk, A.M. (2011). A fast enhanced algorithm of PRI transform. *Int. Symp. on Par. Comput. Elect. Eng.*, pp. 179-184.

Mahmoud, K., Mansour, P.A. & Farouhar, F. (2012). A new method for detection of complex pulse repetition interval modulations. *Proc. ICSP, Vol. 3*, pp. 1705-1709.

Mardia, H.K. (1989). New techniques for the deinterleaving of repetitive sequences. *Proc. RSP, Vol.6*, pp. 149-154.

Milojevic, D.J. & Popovic, B.M. (1992). Improved algorithm for the deinterleaving of radar pulses. *Proc. RSP, Vol. 13,* pp. 98-104.

Nishiguchi, K. (2005). Time-period analysis for pulse train deinterleaving. *T. Soc. Inst. Cont. Eng.*, **E-4**: 68-78.

Nishiguchi, K. (2000). Improved algorithm for estimation pulse repetition intervals. *IEEE T. Aero. Elect. Sys.*,**36:** 407-421.

Peizhi, W., Lei, Q. & Hongchao, W. (2012). The sorting of radar pulse signal based on plane transformation. *Int. Conf. Sys. Info.*, pp. 326-328.

Yan, M., Jun, H., Guohua, G. & Xu, Q. (2009). An improved algorithm of PRI transform. *Glob. Congress Int. Sys.*, pp. 145-149.

Yusuf, Z.M., Abbasi, S.S. & Alamoud, A.R.M. (2011). A novel complete set of Walsh and inverse Walsh Transforms for signal processing. *Int. Conf. Comm. Sys. Net. Tech.*, pp. 504-509.

EVALUATION OF THE EFFECT OF GLOBAL POSITIONING SYSTEM (GPS) SATELLITE CLOCK ERROR VIA GPS SIMULATION

Dinesh Sathyamorthy*, Shalini Shafii, Zainal Fitry M Amin, Asmariah Jusoh & Siti Zainun Ali

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

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

ABSTRACT

This study is aimed at evaluating the effect of Global Positioning System (GPS) satellite clock error using GPS simulation. Two conditions of tests are used; Case 1: All the GPS satellites have clock errors within the normal range of 0 to 7 ns, corresponding to pseudorange error range of 0 to 2.1 m; Case 2: One GPS satellite suffers from critical failure, resulting in clock error in the pseudorange of up to 1 km. It is found that increase of GPS satellite clock error causes increase of average positional error due to increase of pseudorange error in the GPS satellite signals, which results in increasing error in the coordinates computed by the GPS receiver. Varying average positional error patterns are observed for the each of the readings. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over location and time, resulting in GPS accuracy being location / time dependent. For Case 1, in general, the highest average positional error values are observed for readings with the highest PDOP values, while the lowest average positional error values are observed for readings with the lowest PDOP values. For Case 2, no correlation is observed between the average positional error values and PDOP, indicating that the error generated is random.

Keywords: *Global Positioning System (GPS) simulation; GPS satellite clock error; pseudorange error; positional errors; position dilution of precision (PDOP).*

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 Global Positioning System (GPS) and *Global'naya Navigatsionnaya Sputnikovaya Sistema* (GLONASS) are the primarily used GNSS systems worldwide, the upcoming Galileo and BeiDou systems 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 frequency 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 (Kaplan & Hegarty, 2006; RAE, 2011; Schue, 2012; Schuster, 2013).

Fundamental to the operation of GNSS is the one-way ranging that depends on GNSS satellite clock predictability. Even though the clocks in GNSS satellites are very accurate, they drift slightly, resulting in small errors that affect GNSS accuracy. This drift can be in the order of 9 to 18 ns per day and introduces a slow ramp type error in the transmitted signal. This error is difficult to detect because

its signature resembles the typical relative motion between a GNSS satellite and receiver. The GNSS control segment continually monitors the satellite clocks and corrects any drift that is found. However, these corrections are based on observations and may not indicate the clock's current state, leaving residual error in the range of up to 7 ns (Olynik, 2002; Kaplan & Hegarty, 2006; Worley, 2007; RAE, 2011; Bidikar *et al*., 2014). On occasion, the satellite clocks behave unpredictably and produce errors that grow significantly before the operators can spot it and mark it as unhealthy. For example, on 1 January 2004, the clock on GPS satellite SV-23 drifted for approximately 3 h by a pseudorange error rate of 70.6 m/s before the command centre marked it as unhealthy, by which time the pseudorange error had grown from 0 to 285 km (Eastlack, 2004). A similar clock failure occurred for GPS satellite SV-22 on 28 July 2001, where its clock drifted for 90 min, leading to pseudorange error of up to 200 km (Lavraks, 2005).

This study is aimed at evaluating the effect of GPS satellite clock error on GPS performance. It will be conducted using GPS simulation, which will allow the tests to be held with various repeatable conditions, as defined by the authors. As the tests are conducted in controlled laboratory environments, they will not be inhibited by unintended signal interferences and obstructions (Aloi *et al*., 2007; Kou & Zhang, 2011; Pozzobon *et al*., 2013). In previous studies, GPS simulation was used to evaluate the vulnerabilities of GPS to radio frequency interference (RFI) (Dinesh *et al*., 2012, 2014a) and multipath (Dinesh *et al*., 2013, 2014b).

2. METHODOLOGY

The apparatus used in the study are an Aeroflex GPSG-1000 GPS simulator (Aeroflex, 2010), a notebook running GPS Diagnostics v1.05 (CNET, 2004) and a Garmin GPSmap 60CSx handheld GPS receiver (Garmin, 2007). The GPS receiver employs the GPS L1 coarse acquisition (C/A) signal, which is an unencrypted civilian GPS signal widely used by various GPS receivers. The signal has a fundamental frequency of 1,575.42 MHz and a code structure which modulates the signal over a 2 MHz bandwidth (DOD, 2001; Kaplan & Hegarty, 2006; USACE, 2011). The study is conducted in STRIDE's mini-anechoic chamber (Kamarulzaman, 2010) to avoid external interference signals and unintended multipath errors. The test setup employed is as shown in Figure 1. Simulated GPS signals are generated using the GPS simulator and transmitted via the coupler. The following assumptions are made for the tests conducted:

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

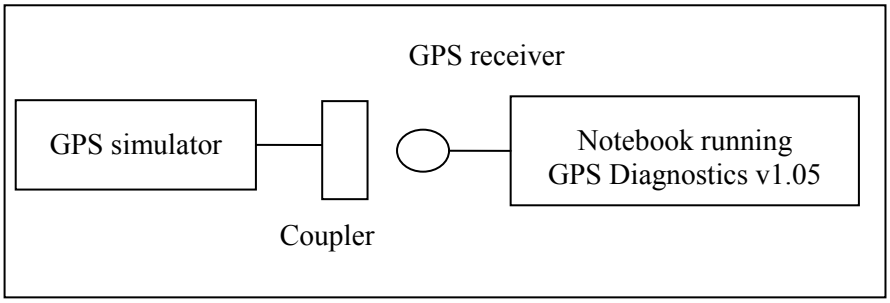


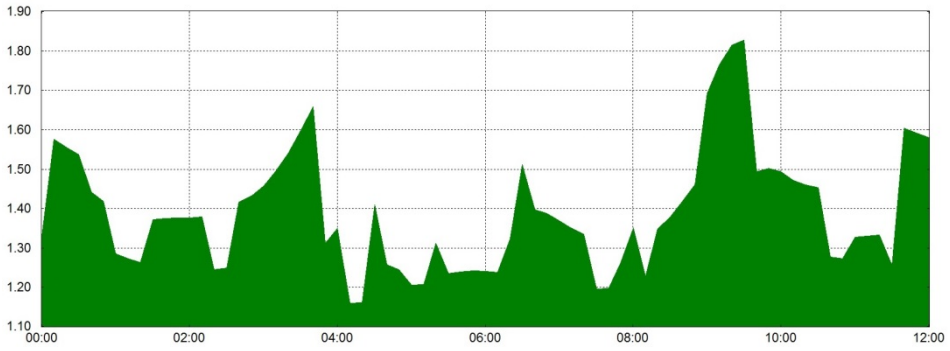
Figure 1: The test setup employed.

The tests are conducted for coordinated universal time (UTC) times of 0000, 0300, 0600 and 0900 for the following coordinates:

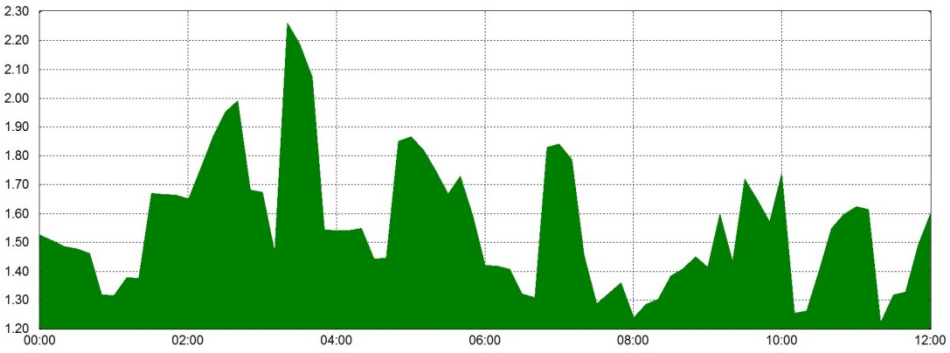
i) N 2° 58', E 101° 48', 0 m (Kajang, Selangor, Malaysia)
ii) N 39° 45', W 105° 00', 0 m (Denver, Colorado, USA)
iii) S 16° 55', E 145° 46', 0 m (Cairns, Queensland, Australia)
iv) S 51° 37', W 69° 12', 0 m (Rio Gallegos, Argentina).

The almanac data for the periods is downloaded from the US Coast Guard's web site (USCG, 2014) and imported into the GPS simulator. The GPS signal power level is set at -130 dBm.

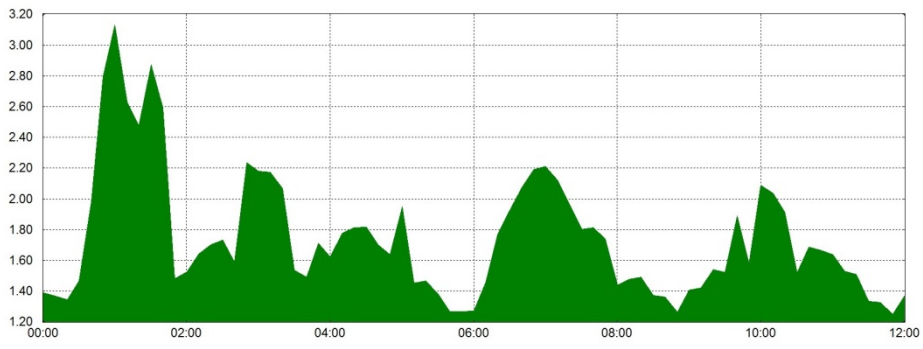
Trimble Planning (Trimble, 2014) is used to estimate GPS satellite coverage at the test areas for the period of the study in terms of position dilution of precision (PDOP) (Figure 2), which represents the effect of GPS satellite geometry on 3D positioning precision. A PDOP value of 1 is associated with 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; Kaplan & Hegarty, 2006; Dinesh *et al*., 2010).



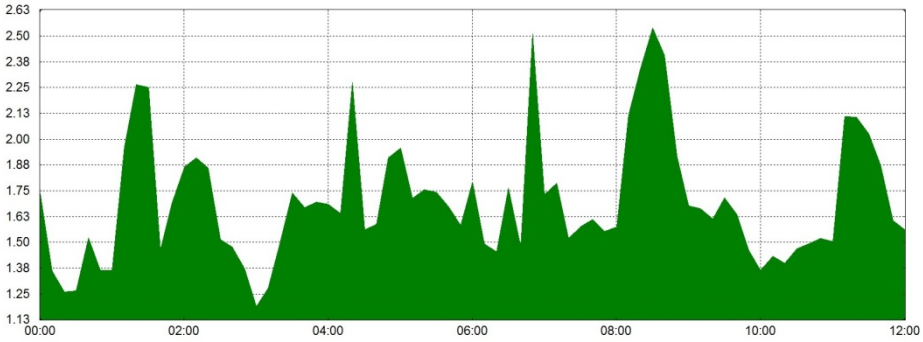
(a)



(b)



(c)



(d)

Figure 2: PDOP of GPS coverage at the test areas for the period of the tests: (a) Kajang (b) Denver (c) Cairns (d) Rio Gallegos. The *x*-axis is UTC time while the *y*-axis is PDOP. (Source: Screen captures from Trimble Planning)

The GPS simulator does not provide specific GPS satellite clock error simulation. However, it does allow for selection of pseudorange errors for the GPS satellites. For this study, GPS satellite clock error is simulated using the pseudorange error function, with 1 ns of clock error representing a pseudorange error of 0.3 m (Olynik, 2002; Kaplan & Hegarty, 2006; Worley, 2007; RAE, 2011; Bidikar *et al*., 2014). Two conditions of tests are used:

- **Case 1:** All the GPS satellites have clock errors within the normal range of 0 to 7 ns, corresponding to pseudorange error range of 0 to 2.1 m.
- **Case 2:** One GPS satellite, with the highest elevation (Table 1), suffers from critical failure, resulting in clock error in the pseudorange of up to 1 km (the maximum pseudorange error provided by the GPS simulator).

Table 1: GPS satellites (SV) with the highest elevation at the start of each test period. These satellites are used to simulate critical failure that causes large clock error.

Location	Time	SV	Elevation	Azimuth
Kajang	0000	16	65.77	-133.38
	0300	3	86.43	-3.87
	0600	1	65.12	103.50
	0900	2	64.45	-37.06
Denver	0000	1	85.27	-35.07
	0300	29	76.79	-48.33
	0600	21	79.92	97.25
	0900	14	72.36	19.84
Cairns	0000	14	87.27	-163.54
	0300	31	63.11	119.28
	0600	11	57.69	-78.83
	0900	20	82.00	37.34
Rio Gallegos	0000	26	72.89	-107.89
	0300	24	73.81	-108.52
	0600	25	79.51	-125.26
	0900	21	63.00	-19.45

For each reading, the coordinates computed by the GPS receiver are recorded for a period of 15 min, and the values of average horizontal, vertical and overall errors are calculated.

3. RESULTS & DISCUSSION

As observed in Figures 3-10, and Tables 2 and 3, increase of GPS satellite clock error causes increase of average positional error. This is due to increase of pseudorange error in the GPS satellite signals, which results in increasing error in the coordinates computed by the GPS receiver. It is observed that the maximum overall error caused by satellite clock error is in the range of 1.42 to 2.40 m for Case 1, and 929.36 to 1,393.98 m for Case 2. For Case 2, the overall errors caused are constrained by the limitation of the pseudorange error function (1 km) provided by the GPS simulator. In comparison, the critical failures suffered by GPS satellites SV-22 in 2001 and SV-23 in 2004 caused pseudorange errors of up to 200 and 285 km respectively (Eastlack, 2004; Lavraks, 2005).

It is observed that for Case 1, for all the readings, the values of vertical error are larger than horizontal error, as the GPS receiver can only track GPS satellites above the horizon, resulting in the vertical solution being less precise than the horizontal solution (DOD, 2001; Kaplan & Hegarty, 2006; USACE, 2011). For Case 2, vertical error is initially larger than horizontal error, but with increasing GPS satellite clock error, horizontal error becomes larger than vertical error. This is as the GPS satellite with simulated critical error has high elevation, causing horizontal error to increase at a higher rate as compared to vertical error. Critical failure simulation applied to GPS satellites with lower elevations would result in higher rate of vertical error increase and lower rate of horizontal error increase.

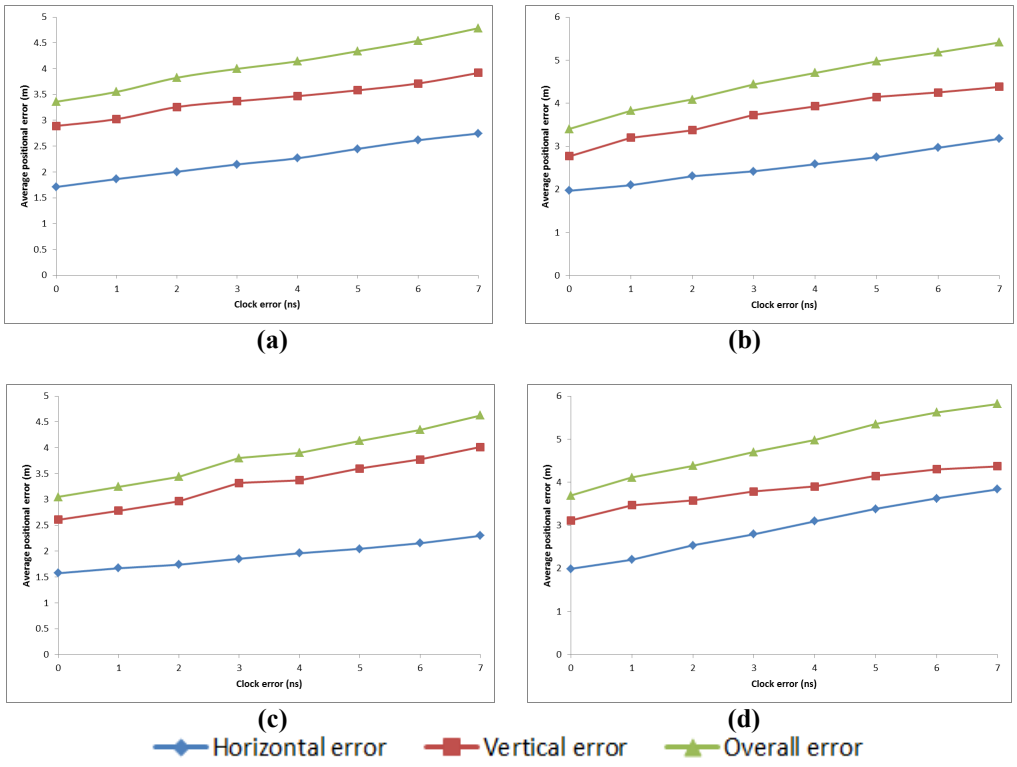


Figure 3: Recorded average positional error values for Case 1 at Kajang for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

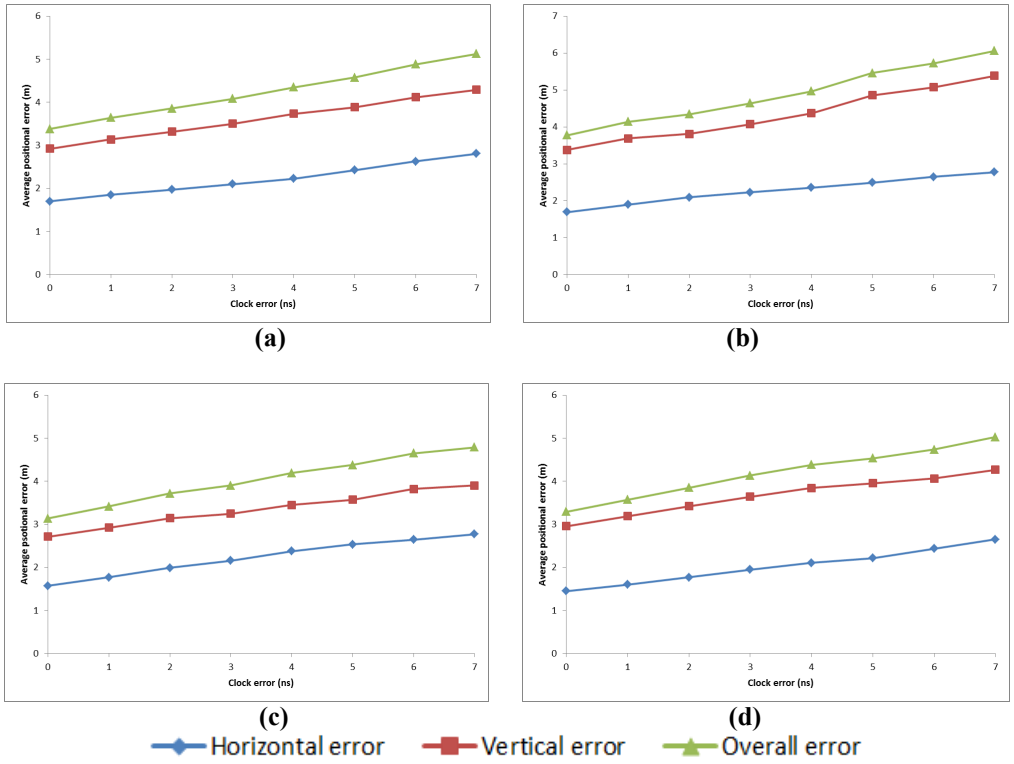


Figure 4: Recorded average positional error values for Case 1 at Denver for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

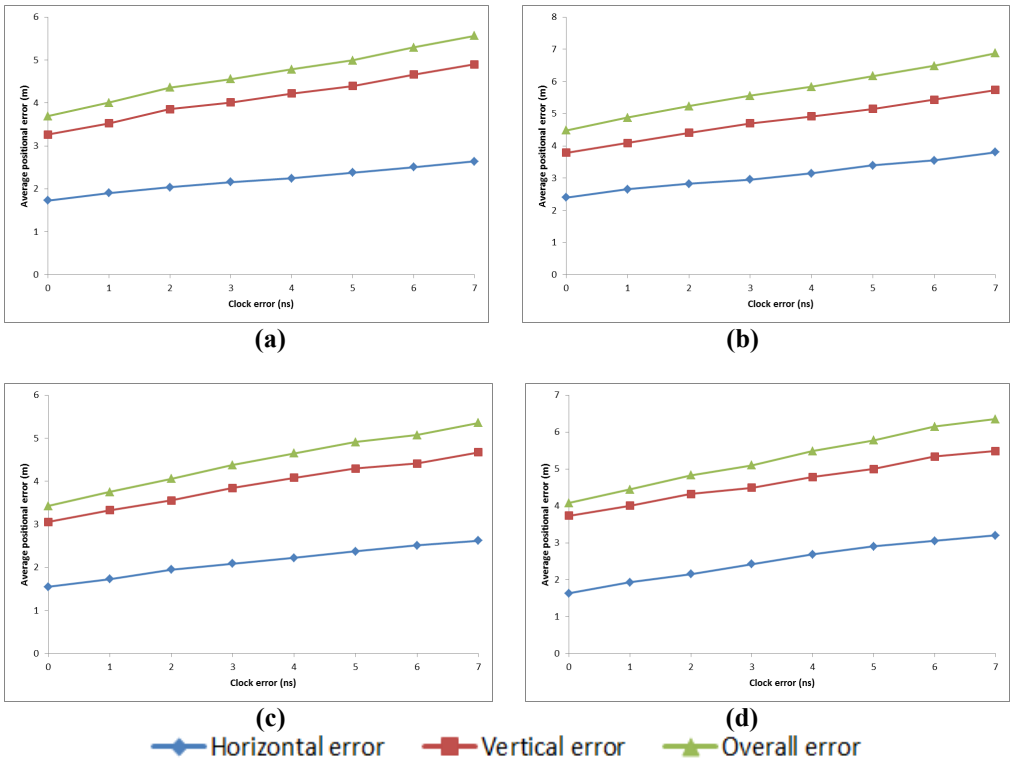


Figure 5: Recorded average positional error values for Case 1 at Cairns for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

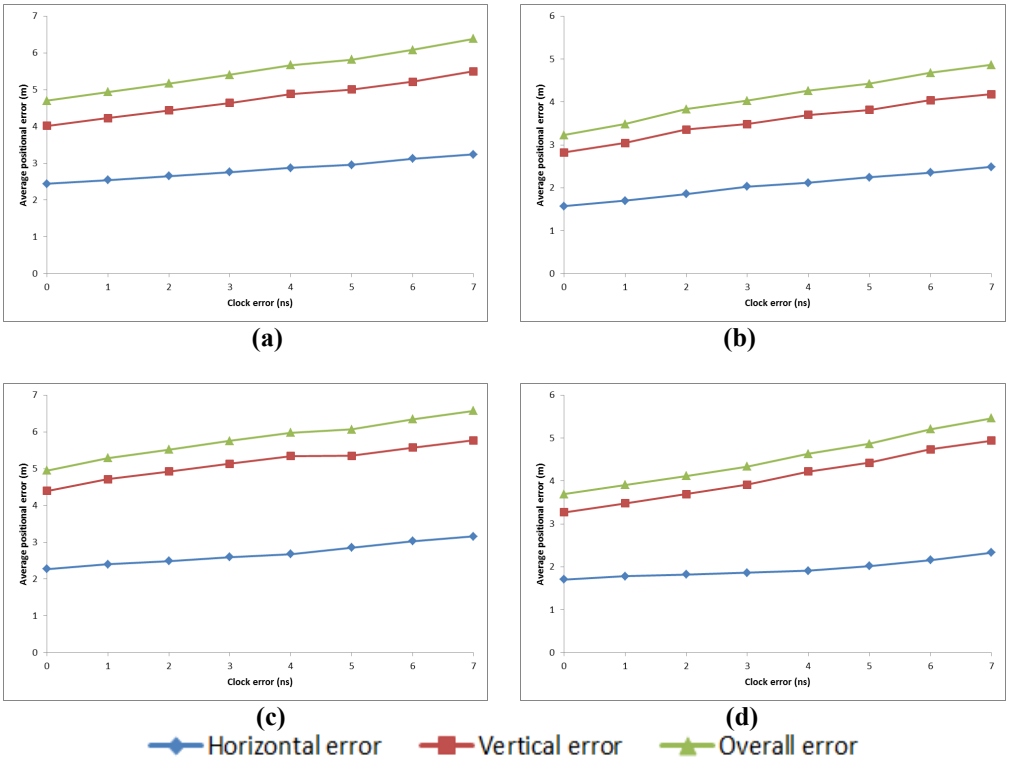


Figure 6: Recorded average positional error values for Case 1 at Rio Gallegos for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

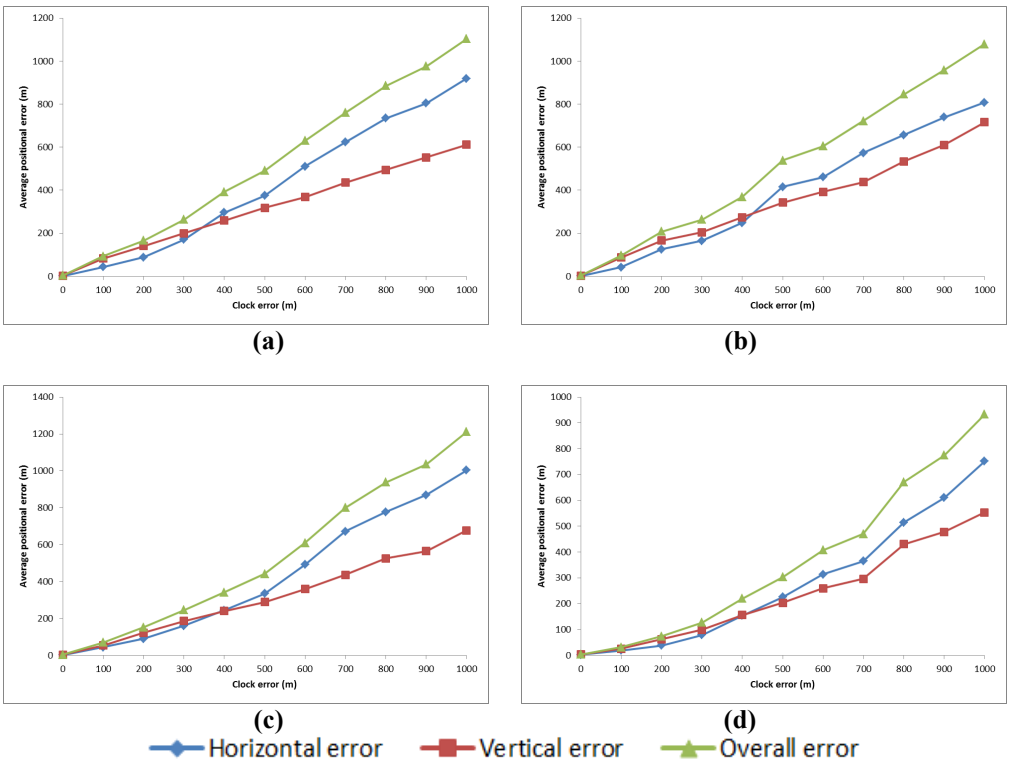


Figure 7: Recorded average positional error values for Case 2 at Kajang for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

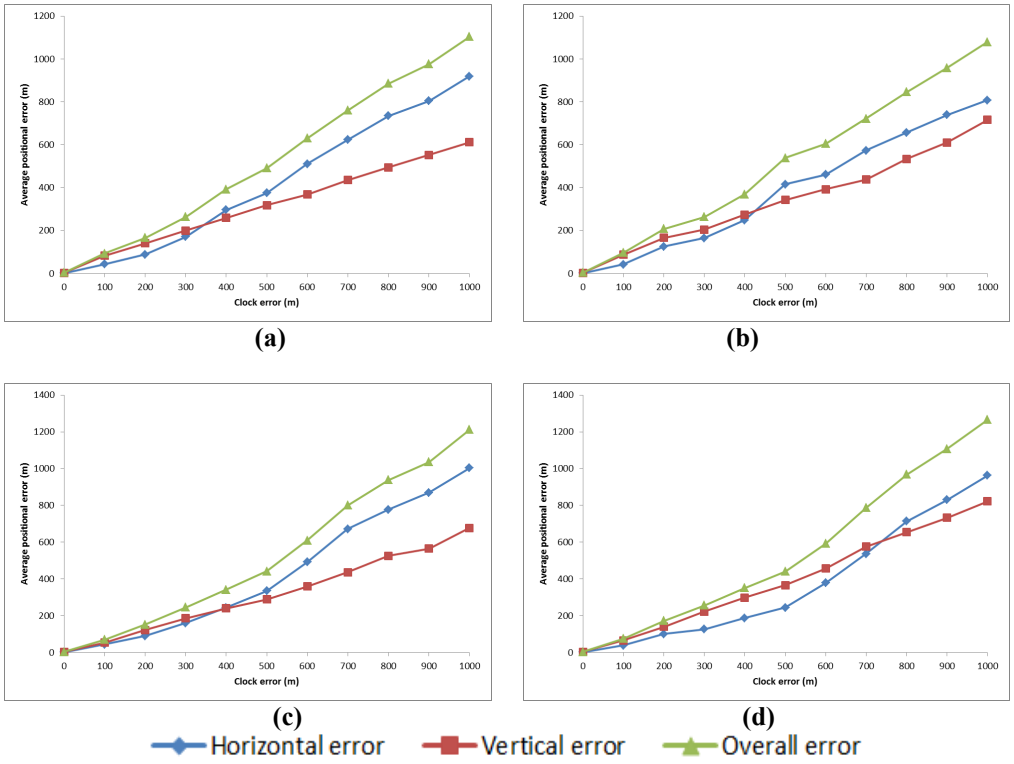


Figure 8: Recorded average positional error values for Case 2 at Denver for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

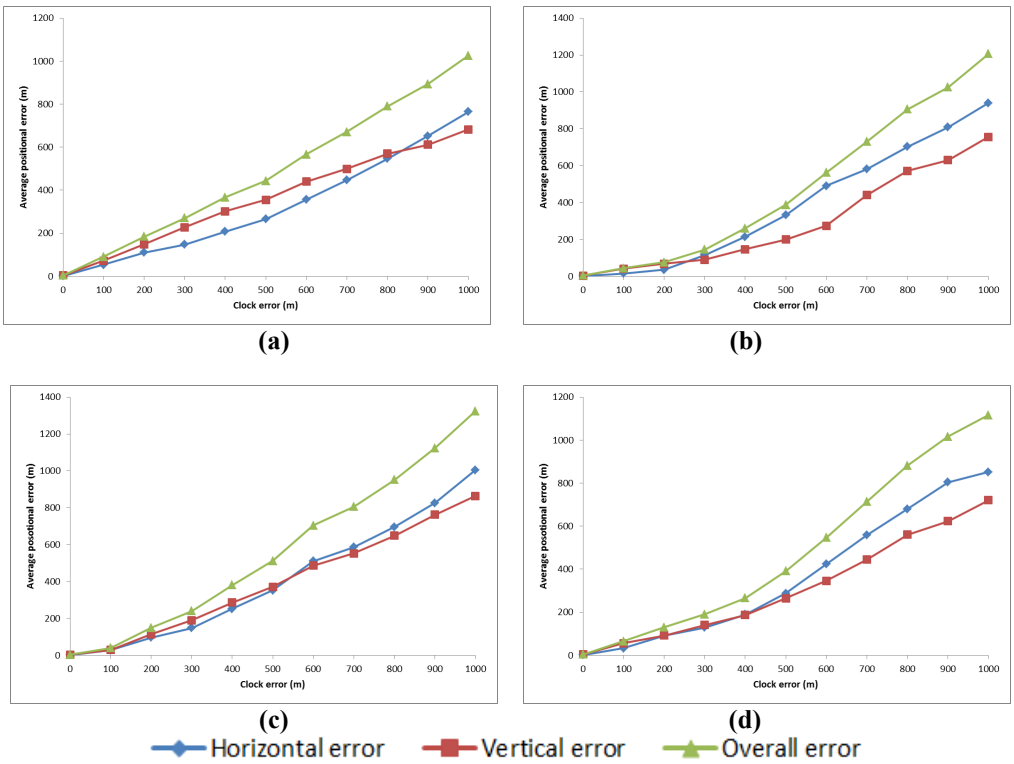


Figure 9: Recorded average positional error values for Case 2 at Cairns for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

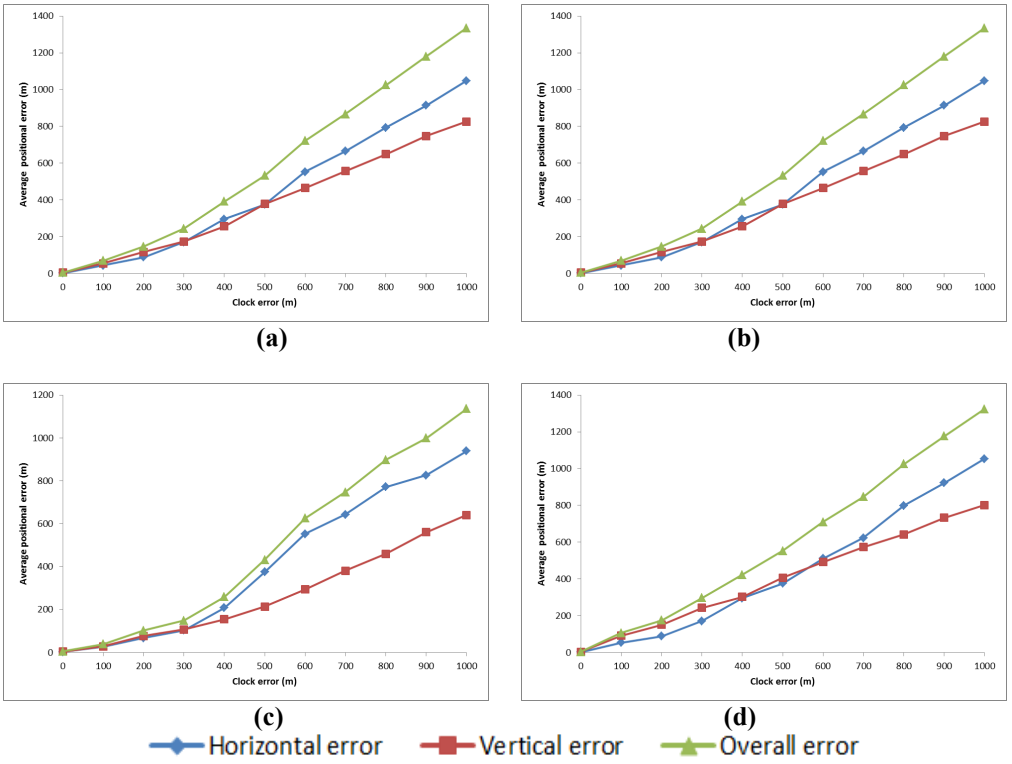


Figure 10: Recorded average positional error values for Case 2 at Rio Gallegos for UTC times of: (a) 0000 (b) 0300 (c) 0600 (d) 0900.

Table 2: Average positional errors for Case 1 for clock errors of 0 and 7 ns, and the differences between the two.

Location	Time	Average Positional Error (m)								
		Clock error = 0 ns			Clock error = 7 ns			Difference		
		H	V	O	H	V	O	H	V	O
Kajang	0000	1.71	2.89	3.36	2.74	3.92	4.78	1.03	1.03	1.42
	0300	1.97	2.77	3.40	3.18	4.38	5.41	1.20	1.61	2.01
	0600	1.57	2.61	3.05	2.30	4.01	4.63	0.73	1.40	1.58
	0900	1.99	3.11	3.70	3.84	4.37	5.82	1.85	1.26	2.12
Denver	0000	1.70	2.92	3.38	2.81	4.29	5.13	1.11	1.36	1.74
	0300	1.69	3.37	3.77	2.78	5.39	6.06	1.08	2.01	2.29
	0600	1.57	2.72	3.18	2.77	3.90	4.79	1.20	1.19	1.65
	0900	1.45	2.96	3.29	2.65	4.27	5.02	1.20	1.31	1.73
Cairns	0000	1.73	3.27	3.70	2.64	4.90	5.56	0.91	1.63	1.87
	0300	2.40	3.79	4.48	3.80	5.73	6.88	1.40	1.95	2.40
	0600	1.55	3.06	3.43	2.62	4.67	5.36	1.07	1.61	1.93
	0900	1.63	3.74	4.08	3.20	5.48	6.35	1.57	1.75	2.27
Rio Gallegos	0000	2.44	4.02	4.70	3.24	5.50	6.38	0.80	1.49	1.68
	0300	1.57	2.82	3.23	2.49	4.18	4.86	0.92	1.35	1.63
	0600	2.27	4.40	4.95	3.16	5.77	6.58	0.89	1.37	1.62
	0900	1.71	3.27	3.69	2.33	4.94	5.46	0.62	1.67	1.77

H: Horizontal error
V: Vertical error
O: Overall error

Table 3: Average positional errors for Case 2 for clock errors of 0 m and 1 km, and the differences between the two.

Location	Time	Average Positional Error (m)								
		Clock error = 0 km			Clock error = 1 km			Difference		
		H	V	O	H	V	O	H	V	O
Kajang	0000	1.71	2.89	3.36	919.01	611.48	1103.85	917.30	608.58	1100.49
	0300	1.97	2.77	3.40	807.42	716.15	1079.25	805.43	713.03	1075.56
	0600	1.57	2.61	3.05	1003.80	677.62	1211.11	1002.23	675.01	1208.06
	0900	1.99	3.11	3.70	750.89	553.36	932.76	748.91	550.59	929.36
Denver	0000	1.70	2.92	3.38	1047.54	924.92	1397.44	1045.84	921.88	1393.98
	0300	1.69	3.37	3.77	960.36	841.95	1277.17	958.67	838.57	1273.40
	0600	1.57	2.72	3.18	916.61	743.82	1180.44	915.036	741.11	1177.30
	0900	1.45	2.96	3.29	962.50	821.22	1265.23	961.05	818.27	1261.94
Cairns	0000	1.73	3.27	3.70	765.25	682.65	1025.49	763.53	679.38	1021.79
	0300	2.40	3.79	4.48	939.41	755.62	1205.59	937.01	751.84	1201.11
	0600	1.55	3.06	3.43	1003.95	863.48	1324.20	1002.40	860.42	1320.78
	0900	1.63	3.74	4.08	852.32	720.22	1115.87	850.69	716.49	1111.80
Rio Gallegos	0000	2.44	4.02	4.70	1047.54	826.48	1334.32	1045.10	822.46	1329.62
	0300	1.57	2.82	3.23	1003.95	761.95	1260.35	938.23	641.12	1136.36
	0600	2.27	4.40	4.95	938.23	641.12	1136.36	935.96	636.73	1131.41
	0900	1.71	3.27	3.69	1053.26	801.62	1323.62	1051.55	798.35	1319.93

H: Horizontal error
V: Vertical error
O: Overall error

Varying average positional error patterns are observed for the each of the readings. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over location and time, resulting in GPS accuracy being location / time dependent (DOD, 2001; Kaplan & Hegarty, 2006; Dinesh *et al*., 2010). For Case 1, in general, the highest average positional error values are observed for readings with the highest PDOP values (Kajang at 0900, Denver at 0300, Cairns at 0300 and Rio Gallegos at 0600), while the lowest average positional error values are observed for readings with the lowest PDOP values (Kajang at 0600, Denver at 0600, Cairns at 0600 and Rio Gallegos at 0300). For Case 2, no correlation is observed between the average positional error values and PDOP, indicating that the error generated is random.

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 carrier-to-noise density (C/N_0) levels, which is the ratio of received GPS signal power level to noise density. Lower C/N_0 levels would 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, higher rates of increase of positional error values (DOD, 2001; Kaplan & Hegarty, 2006; Petovello, 2009; USACE, 2011).

4. CONCLUSION

Based on the results of this study, it was found that increase of GPS satellite clock error caused increase of average positional error due to increase of pseudorange error in the GPS satellite signals, which resulted in increasing error in the coordinates computed by the GPS receiver. Varying average positional error patterns were observed for the each of the readings. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over location and time, resulting in GPS accuracy being location / time dependent. For Case 1 (all the GPS satellites have clock errors within the normal range of 0 to 7 ns), in general, the highest average positional error values were observed for readings with the highest PDOP values, while the lowest average positional error values were observed for readings with the lowest PDOP values. For Case 2 (one GPS satellite suffers from critical failure, resulting in clock error in the pseudorange of up to 1 km), no correlation was observed

between the average positional error values and PDOP, indicating that the error generated was random.

REFERENCES

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

Aloi, D.N., Alsliety, M. & Akos, D.M. (2007). A methodology for the evaluation of a GPS receiver performance in telematics applications. *IEEE T. Instrum. Meas.*, **56**: 11-24.

Bidikar, B., Rao, G.S., Ganesh, L. & Kumar, M.S. (2014). Satellite clock error and orbital solution error estimation for precise navigation applications. *Positioning*, **5**: 22-26.

CNET (2004). *GPSDiag 1.0*. Available online at: http://download.cnet.com/GPSDiag/3000-2130_4-4951103.html (Last access date: 31 January 2010).

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. & Zainal Fitry, M.A. (2012). 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., Shalini, S., Zainal Fitry, M.A. & Siti Zainun, A. (2013). Evaluation of the repeatability of Global Positioning System (GPS) performance with respect to GPS satellite orbital passes. *Defence S&T Tech. Bull.*, **6**: 130-140.

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 Hisam, M.Y. (2014a). Evaluation of the effect of radio frequency interference (RFI) on Global Positioning System (GPS) receivers via GPS simulation. *ASM Sci. J.*,**8**: 11-20.

Dinesh, S., Shalini, S., Zainal Fitry, M.A., Siti Zainun, A., Siti Robiah, A., Mohd Idris, I. & Mohd Hasrol Hisam, M.Y. (2014b). Evaluation of the effect of commonly used materials on multipath propagation of Global Positioning System (GPS) signals via GPS simulation. *Adv. Mil. Tech.*, **9**: 81-95.

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

Eastlack, H. (2004). *SVN-23/PRN-23 Integrity Failure of 1 January 2004*. Second Space Operations Squadron, US Air Force, Washington, D.C.

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

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

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

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

Lavraks, J.W. (2005). *An Overview of Civil GPS Monitoring*. Institute of Navigation (ION), Manassas, Virginia.

Olynik, M.C. (2002). *Temporal Characteristics of GPS Error Sources and Their Impact on Relative Positioning*. Master's thesis, The University of Calgary Calgary, Alberta.

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

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.

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

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

Schuster, W. GNSS vulnerabilities: Providing maximum user protection. *7th Annu. GNSS Vulnerabilities Sol. Conf.*, 18-20 April 2013, Baska, Croatia.

Trimble (2014). *Trimble's Planning Software*. Available online at: http://www.trimble.com/planningsoftware.shtml (Last access date: 31 July 2014).

USACE (US Army Corps of Engineers) (2011). *Engineer Manual EM 1110-1-1003: NAVSTAR Global Positioning System Surveying.* US Army Corps of Engineers (USACE), Washington D.C.

USCG (US Coast Guard) (2014). *GPS NANUs, Almanacs, & Ops Advisories*. Available online at: http://www.navcen.uscg.gov/?pageName=gpsAlmanacs (Last access date: 31 July 2014).

Worley, S. (2007). *GPS Errors & Estimating Your Receiver's Accuracy*. Available online at: http://edu-observatory.org/gps/gps_accuracy.html (Last access date: 31 July 2014).

NETWORK PROBE PATTERNS AGAINST A HONEYNET IN MALAYSIA

Nogol Memari*, Shaiful Jahari Hashim & Khairulmizam Samsudin

Department of Computer and Communication Systems Engineering, Faculty of Engineering, University Putra Malaysia (UPM), Malaysia

*Email: nogolmemari@gmail.com

ABSTRACT

In this paper, a honeynet is deployed with the help of container based virtualisation technology to gain comprehensive information on the actions against the network. The honeynet is deployed using a University Putra Malaysia (UPM) specific internet protocol (IP) address to attract attention from internet users and network data is then gathered from the scans performed on the honeynet for a period of two weeks. The data is then analysed to determine the patterns of activity based on port scans, Secure Shell (SSH) connection attempts and the variety of operating systems where the attacks initiated from. Windows XP was found to be the primary choice for infection by the hackers as Microsoft stopped issuing security updates for this particular platform, while Linux systems are less infected due to frequent security upgrades. Interestingly, US and Russian based IP addresses poked the SSH server the most, followed by Malaysian IP addresses.

Keywords: *Network security; honeynet; virtualisation; Linux containers (LXC); low- and high-interaction honeypots.*

1. INTRODUCTION

Since the beginning of the internet, network security has been a major concern for software developers and hardware vendors. The number of serious cyber-attacks detected over the last two years has increased so much that new attacks rarely cause much surprise. According to Kaspersky (2014), 91% of the organisations polled suffered a cyber-attack at least once in 2013, while 9% were victims of targeted attacks. Figure 1 depicts the rate of cyber-attacks specified in different categories. With passing time, a number of security solutions, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), antiviruses and firewalls have become popular (Provos & Holz 2007; Li *et al*., 2008; Benzel *et al*., 2009). These kinds of security solutions mainly focus on protecting computers and networks against vulnerabilities. Honeynet technology offers a comprehensive solution to spy on intruders and deceive them from not using the resources, and to monitor them while they attack the network (Joshi & Sardana 2011). A honeynet is combination of electronic decoys, namely honeypots, which has the capability of monitoring and analysing intruders to study their behaviour in order to protect the system from further attacks (Bao *et al*., 2010; Albin, 2011).

In this paper, a honeynet consisting of both low- and high-interaction honeypots is deployed to study the network scan patterns against a University Putra Malaysia (UPM) specific internet protocol (IP) address. The honeynet is placed before the firewall of the university to provide better access to the internet. The designed honeynet was connected to the internet for a period two weeks. When it was connected, more than thousands of Secure Shell (SSH) and transmission protocol scans were performed against the deployed honeynet.

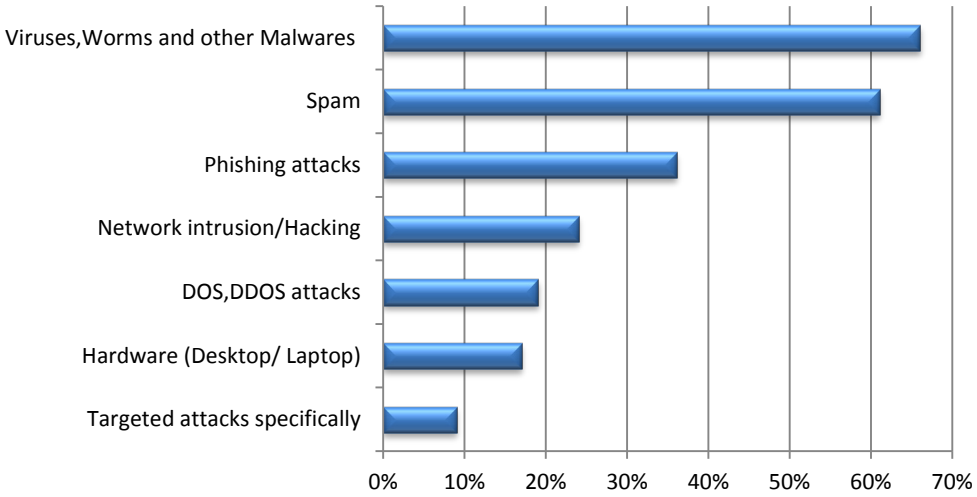


Figure 1: Rate of cyber-attacks in 2013.
(Source: Kaspersky (2014))
***DOS stands for Denial of Service. DDOS, or Distributed Denial of Service, is a more complex breach in the same category**

2. HONEYPOT AND HONEYNET

A honeypot is an electronic decoy designed to be compromised for the purpose of collecting information from an intruder, such as tools, motives, patterns and methods that are used by attacker (Honeynet, 2014). The intelligence gathered on intrusion patterns and technologies can improve the knowledge on defensive mechanisms and set new rules to strengthen security systems. Honeypots can be categorised based on the level of their interaction with attackers and the purpose of deploying them (Yeh & Yang 2008; Liu *et al*., 2011; Kaur *et al*., 2012).

2.1 Low- and High-Interaction Honeypots

Low-interaction honeypots are systems that simulate network services with the help of software and pretend to be affected by the existence of active components, such as Telnet or Hyper Text Transfer Protocol (HTTP) servers. Since the emulated services do not offer full functionality, it is possible to implement services belonging to different operating systems on one honeypot (Mokube & Adams, 2007; Honeynet, 2014).

High-interaction honeypots are commercial off-the-shelf computers. Unlike a low-interaction honeypot, they run actual operating systems and fully functional services, just like in a productive environment. Therefore, high-interaction honeypots are hard to distinguish from a normal computer connected to the Internet (Provos & Holz, 2007). Figure 2 provides a comparison between low- and high-interaction honeypots.

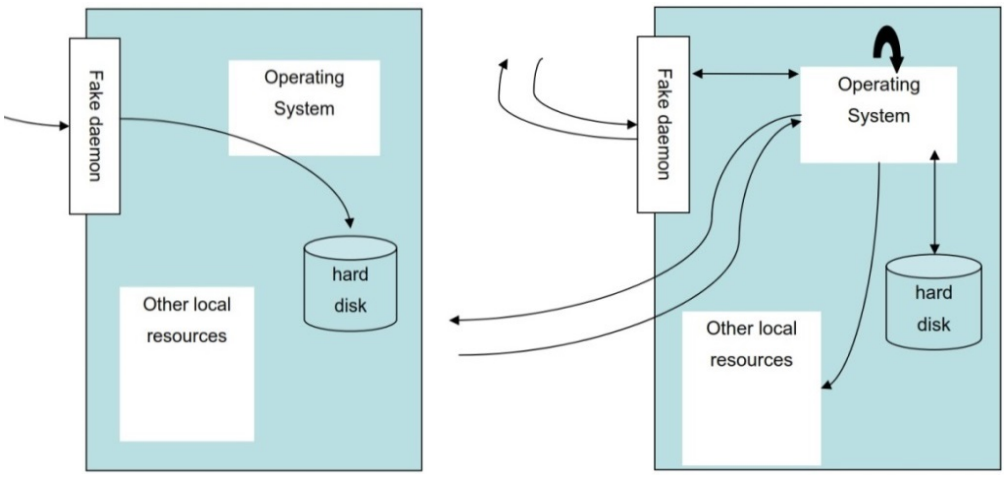


Figure 2: (a) Low- and (b) high-interaction honeypots.
(Source: Provos and Holz (2007))

2.2 Production and Research Honeypots

Production honeypots are those which are used by organisations to protect them and to help them in mitigating risk. They are considered to be valuable because they provide security to any production resources. Production honeypots are easier to build, deploy and maintain as they require less functionality than research honeypots. By using production honeypots, we may know where the source of attacks are and which exploits are carried out. Production honeypots are deployed in such a way that they mirror the production servers or any service for the attackers to work with and to expose any vulnerability present in the network (Vrable *et al*., 2005; Abbasi & Harris 2009; Honeynet 2014).

Research honeypots normally do not add any direct value to the organisation. Instead they are designed to gather information about the back-hat community. Organisations like government agencies, defence institutions, universities and large corporations use research honeypots to collect information about the threats they face. The focus of research honeypots is to gather intrusion pattern and technologies by intelligence, and to understand the ways and means used by the attackers during an attack. This information is useful to determine the actions, intentions and, sometimes, details of the attackers. Research honeypots are both complex to deploy and to maintain. They can gather large amount of data and can be time-consuming from the administration aspect (Provos & Holz 2007; Abbasi & Harris 2009; Liu *et al*., 2011).

2.3 Honeynet Technology

Honeynet is a group of honeypots that are set up and interconnected behind a special gateway, namely honeywall, with monitoring and filtering capabilities. As such, a separated and highly controlled environment can be created as indicated. Similar to a honeypot, a honeynet lies as a trap to be probed, attacked by the malicious attackers and compromised. However, in comparison to a single system, information collected on threats is more comprehensive and hence, more valuable. On the other hand, the level of complexity is significantly higher. That is why certain guidelines have been proposed in order to safely deploy a honeynet (Awad & Derdmezis, 2005; Nikkhahan *et al*., 2009; Gani, 2012).

3. MATERIALS AND METHODS

Figure 3 illustrates the flow of the deployed honeynet system in detail. The traffic from the internet comes through the Honeywall gateway for data control, capture and analysis. The honeywall, based on the preconfigured rules, will then forward or drop the packet, and logs all activities. It was connected securely through the Secure Sockets Layer (SSL) to the management interface for administration purposes (Musca *et al*., 2013). Data control works with iptables and IPS, namely Snort-inline, and data capture benefits from the standard honeynet loggings system (Qassrawi & Hongli, 2010). All captured data is analysed with the honeywall analyzer, Snort (Caswell & Beale 2004; Snort, 2014) and Wireshark (Wireshark, 2014).

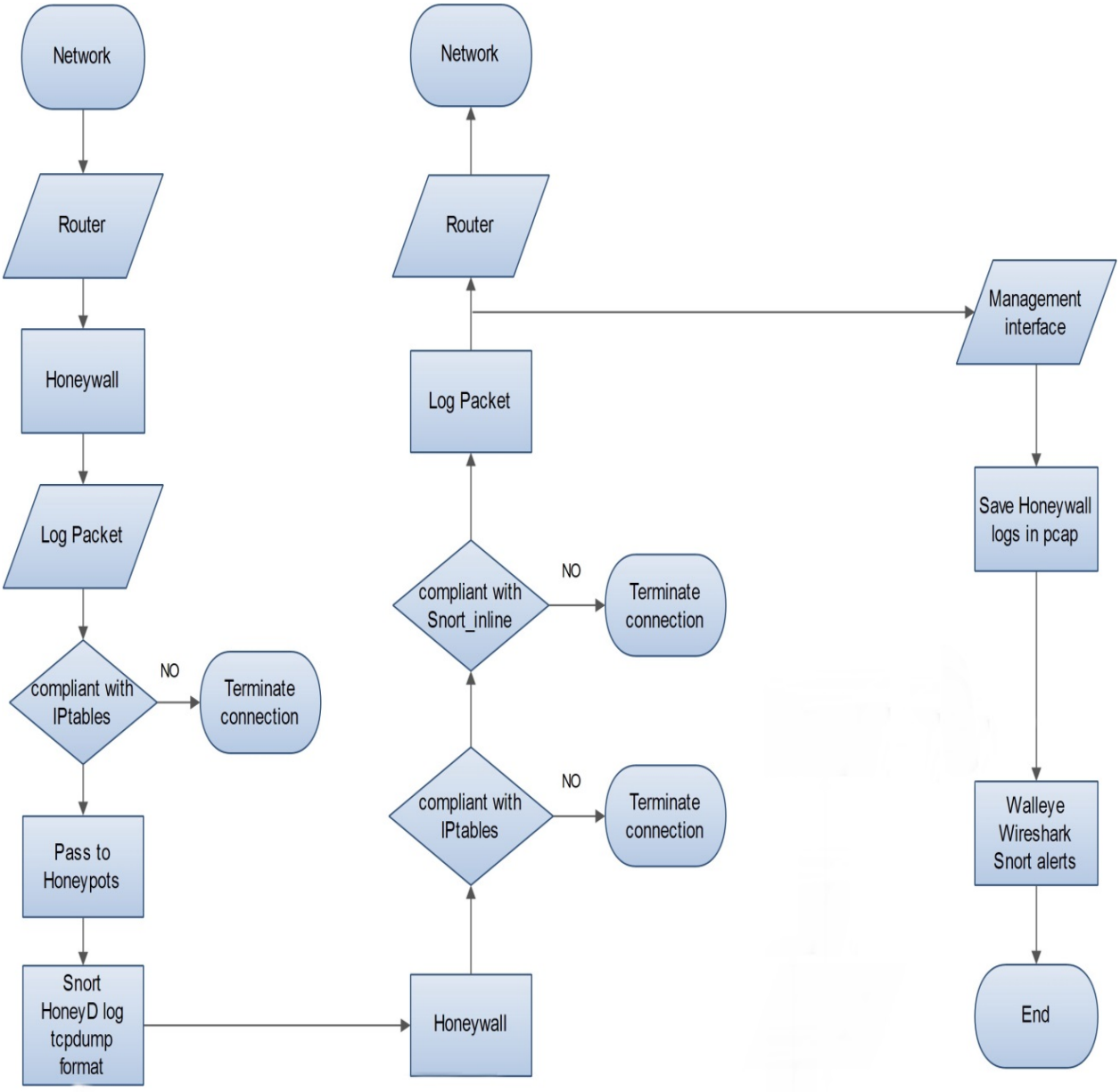


Figure 3: Flowchart of the network interactions of the deployed virtual honeynet.

3.1 Virtualisation and LXC

Virtualisation is the technology that allows one computer to simultaneously exist inside another computer. It also gives a large amount of flexibility to its users, allowing them to use virtual machines (VMs) from anywhere (Binu & Kumar, 2011). This flexibility also gives researchers the possibility to develop their own virtual test-beds that can be created when needed, and easier to maintain, removing the waiting time for hardware (Gurav & Shaikh 2010; Terzo & Vipiana 2012). Linux container (LXC) virtualisation (LXC, 2014) is an operating system level virtualisation that shares the same kernel to manage resource isolation. All the processes can have their own process identification (ID) and their own private view of operating system (Xavier *et al*., 2013; LXC 2014). LXC virtualisation is used in this study to deploy the honeynet.

3.2 Description and Architecture of the Deployed Honeynet

In the deployed honeynet, Honeywall runs on a dedicated machine in order to gain several benefits. Firstly, the implementation will be more secure, because the data capture and analysis is physically isolated from the electronic baits. Thus, even if an attacker successfully compromises a virtual machine, the risk of getting privileged access to the honeynet gateway is comparatively small. Secondly, data control, capture and analysis operate independently from the honeypots. Consequently, the performance level is not reduced if additional decoys are installed, and physical resources must be shared between a higher numbers of VMs (Kaur *et al*., 2012; Honeynet 2014). The virtual honeynet architecture shown in Figure 4 is chosen to deploy our experiment. The devices and services that are used to deploy the honeynet are specified in Table 1.

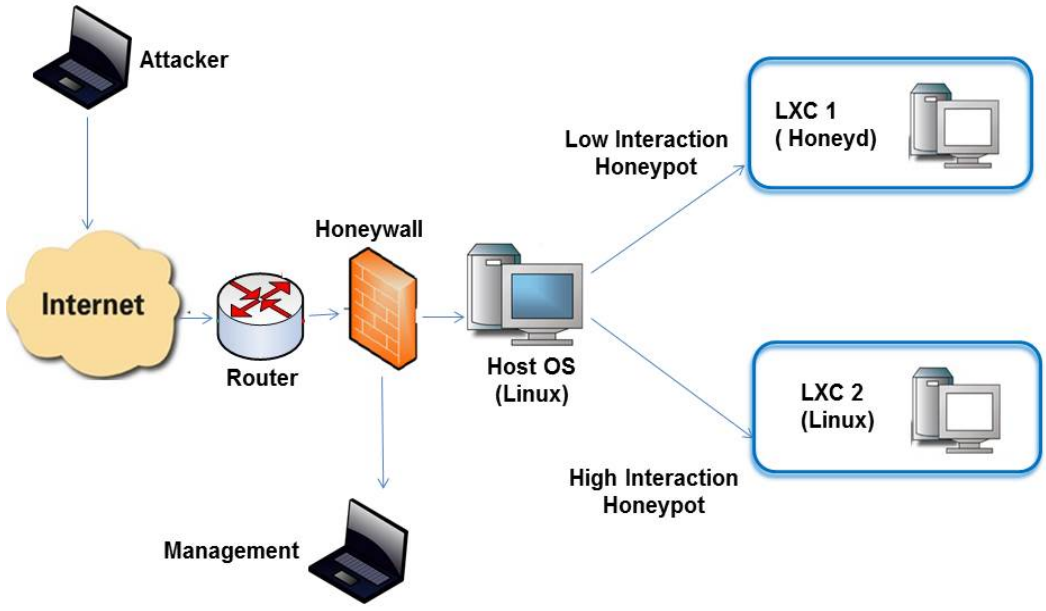


Figure 4: Architecture of the deployed Virtual honeynet.

Table 1: Specifications of the devices and services that are used to deploy the honeynet.

Software tools, OS	Description	Specifications
Linux, Ubuntu 12.04 LTS	Host machine, physical machine	HP ProLiant DL160 server Processors: 8-cores Intel Xeon L5630 @ 2.13 GHz RAM: 4GB;Hard disk:300GB;2 network interface card
Windows 7 Professional	Remote management machine	Lenovo G475 CPU:AMD E450 Network: host-only vboxnet0 (public IP)
Linux, Honeywall Roo (CENTOS 6)	Virtual machine, honeywall gateway for honeypots	Roo 1.4 on pc with: RAM:512MB ; HardDisk:40GB Network:3 [2 bridged(eth0,eth1),1 host- only(eth2)]
LXC running Ubuntu 12.04 LTS	Virtual hybrid honeypot, High interaction honeypot (Include web server) LXC: Virtualization solution, Container	Each LXC uses approximately 200 Mb of hard disk Apache2, PHP5, MySQL and PHP myadmin were installed on each LXC
LXC running Ubuntu 12.04 LTS With Honeyd Emulator	Virtual hybrid honeypot, Low-interaction honeypot (Honeyd)	Honeyd 1.5c were installed on it. Emulated OS: Windows 7 and Windows XP sp3.
Snort inline	IPS	Snort inline 2.6.1.5
Snort (IDS) and Honeyd Log	Data capture tool	Snort 2.9.6.0
Wire shark	Data analysis tool	Version 1.10.6
Walleye Web Interface	Web based graphical user interface (GUI) for configuration, administration and data analysis	Walleye-1.2.1

3.3 Determining Proper Operating Systems for the Honeypots

To choose the proper operating system for both the low- and high-interaction honeypots, the desired design and available software / hardware are considered. In 2013, there has been an overall increase in the number of security flaws discovered in all modern operating systems. As can be seen in Figure 5, the most lucrative target for hackers in 2013 was Linux Kernel, with 22% of all attacks. Windows 7 was the second most vulnerable operating system with 14%. Windows Server 2003, Ubuntu Linux and Mac OS X had approximately a tenth of the entire vulnerable quota (ZDNet, 2014). Since Windows XP's official support from Microsoft just ended in 2013, most attackers will target vulnerable Windows XP systems exposed to the Internet. The low-interaction honeypot is implemented using Honeyd (Provos 2003), emulating both Windows 7 and Windows XP SP3 operating systems, while the high-interaction honeypot emulates the Linux operating systems.

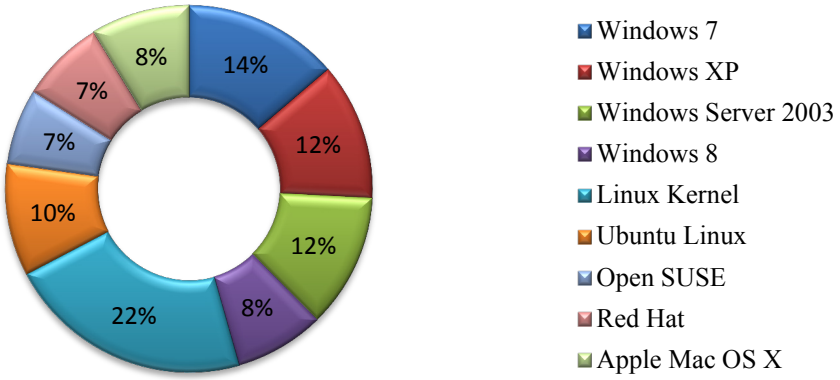


Figure 5: Most attacked and vulnerable operating systems in 2013. (Source: ZDNet (2014))

3.4 Configuring the Virtual Honeypots

The virtual low-interaction honeypot is configured by utilising Honeyd, which is a Linux daemon, a program that runs independently in the background and creates a virtual host on a network, offering arbitrary services. The virtual host can be configured to appear as a particular operating system, thus allowing a personalised setup to fit the user needs. Honeyd has powerful features to run services through scripts that could be configured to go beyond simple port listening and give responses to intruders. Honeyd software provides two types of logs that are used for analysis. Network packet-level logging gives an overview or details of what kind of traffic the honeypots receive, and system logging gives more detailed information about the ongoing traffic. Honeyd can be used for two purposes: distracting potential hackers or catching them in a honeypot. Either way, the hackers will be slowed down and subjected to analysis (Wang & Zeng 2011; Singh & Joshi 2011).

The virtual high-interaction honeypot was deployed with Ubuntu 12.04 on the LXC container. Ubuntu was used because this operating system is one of the most widely used in the Linux distribution. In addition, some vulnerable applications and services, such as MySQL, SSH, Apache2 web server and PHP5 were installed to attract more intruders. Figure 6 shows a web server installed on the high-interaction honeypot to attract more attackers by imitating real services and resources.

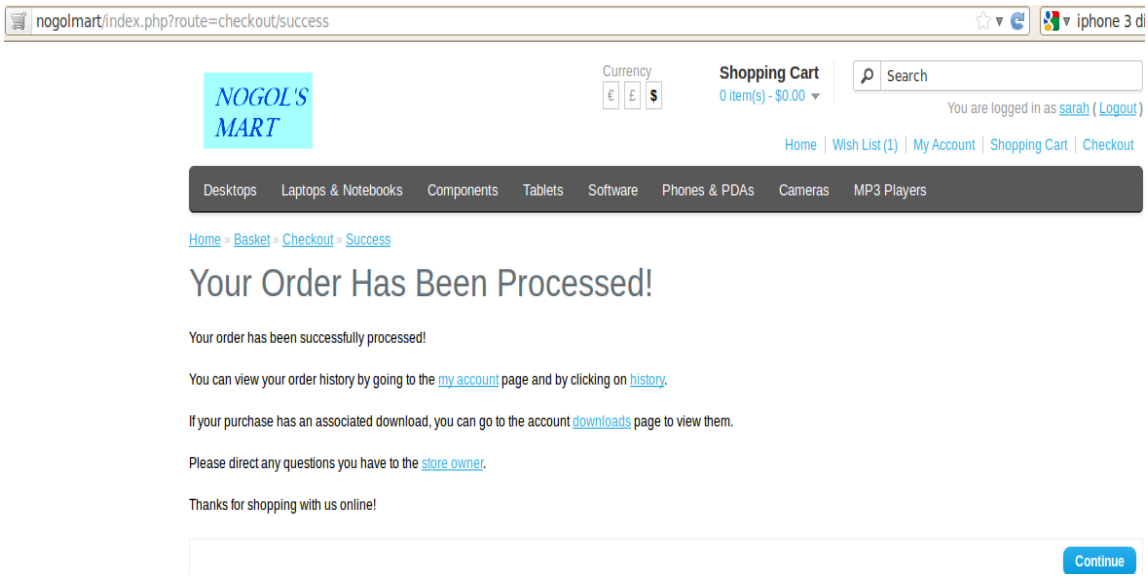


Figure 6: High-interaction honeypot website when processing an order.

The honeypots are placed behind a special physical machine running Roo software, which is the honeywall. The honeywall acts as a transparent network bridge between the Internet and the honeynet (Provos & Holz, 2007; Honeynet 2014). In order to reduce the risk of deploying a honeynet, the honeywall can do either data control, capture and analysis. Roo is capable of monitor and record probes in honeypots and it has special analyser namely walleye for analysing and classifying captured data. Table 2 summarises the mentioned frameworks.

Table 2: Specifications of the deployed honeynet.

Framework	Description
Honeywall	A physical machine acting as a transparent network bridge between the Internet and the honeynet for improved security.
Roo	Honeywall software that needs to be installed on a hard disk. Roo is not a Live-Linux distribution and needs to be configured after installation.
Walleye	Honeywall runs a webserver over SSL to visualise the collected information and it has the capability of analysing data.

4. RESULTS AND DISCUSSION

This section describes the analysis of the attack patterns found on the honeypots and presents an overall statistical analysis of the results gathered from the honeynet. The honeynet was online for a period of approximately two weeks. During this period, over one million probes were received from various countries for instance European countries, United States and Asian countries. These results provide better insight to the readers about what was observed in our honeynet experiment.

Figure 7 shows the ratio of different probe connections during the observation period. It is observed that Transmission Control Protocol (TCP) is the most used protocol by attackers. This can be explained by the fact that multiple services and applications use TCP as compared to other protocols. Both User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) have approximately the same probe pattern in the honeynet probes.

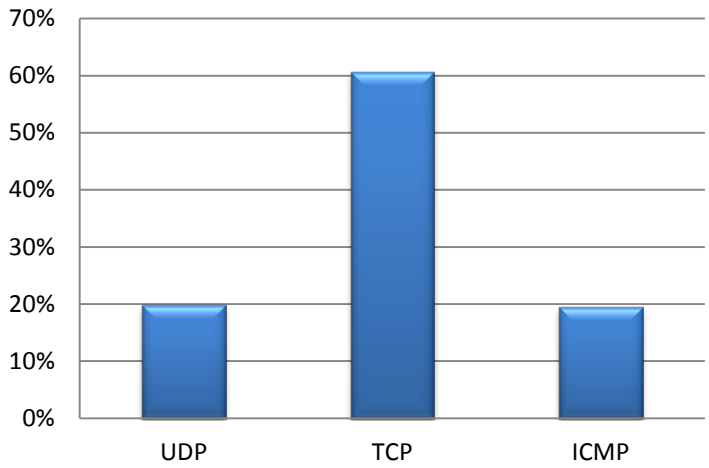


Figure 7: Ratio of overall User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Internet Control Message Protocol (ICMP) scans performed on the honeynet.

A breakdown of the top attacks originating from Linux computers can be seen in Figure 8, while the breakdown of attacks originating from Windows XP and other variants of Windows based systems can be seen in Figures 9 and 10 respectively.

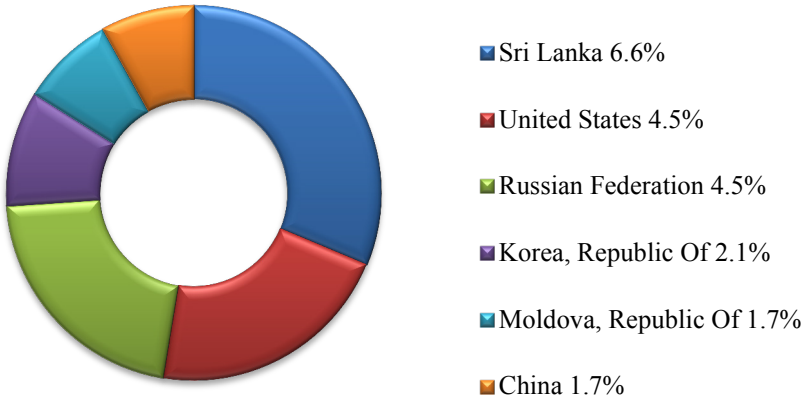


Figure 8: Top attacks originating from Linux computers.

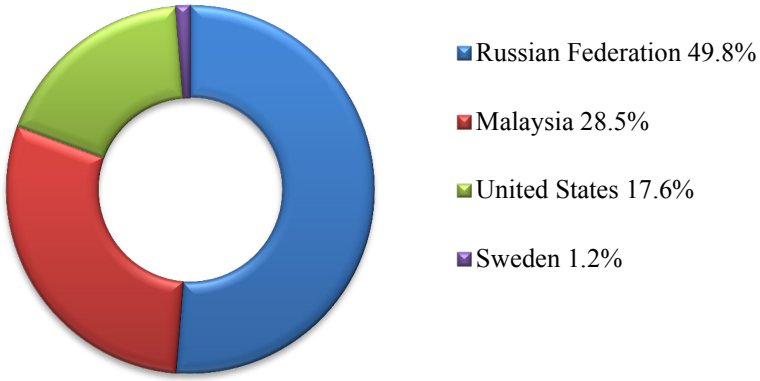


Figure 9: Top attacks originating from Windows XP computers.

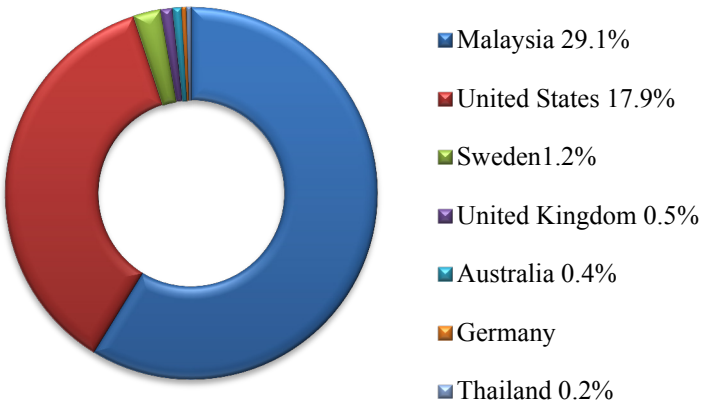


Figure 10: Top attacks originating from other Windows computers.

Figure 11 illustrates comparison of operating systems detected in honeypots. Most of the attacks on our honeynet originated from systems running different variations of Windows operating systems (mostly XP and Windows Server variations). Interestingly, like the systems observed in other honeynet projects, the majority of the attacks were performed by using Windows. This result is coherent with the same measures reported by the Italian (Marchese *et al*., 2011) and Philippine (Philippine Honeynet, 2014) honeypot projects.

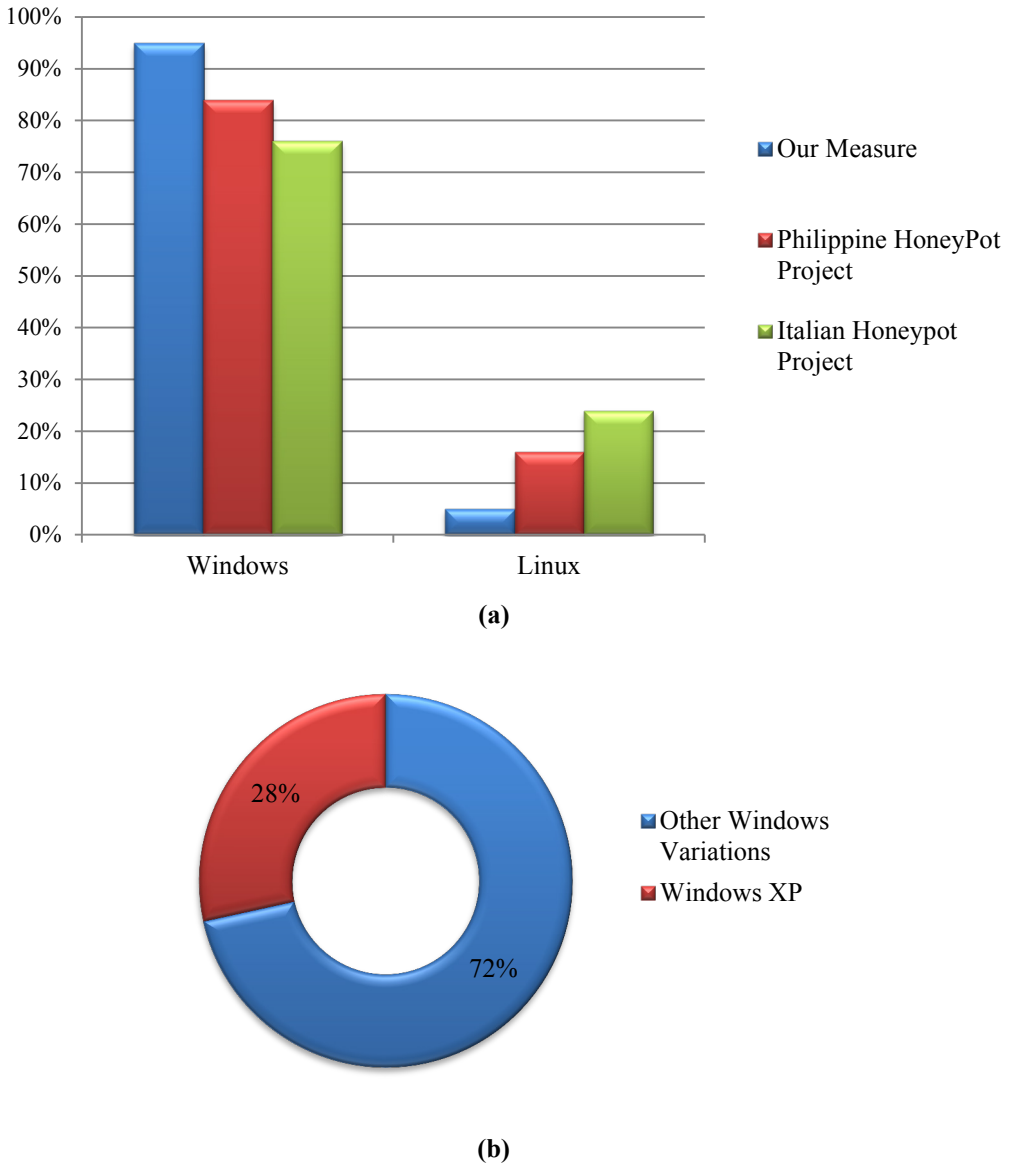


Figure 11: (a) Ratio of operating systems used to initialise scans compared to the Philippine (Philippine Honeynet (2014)) and Italian (Marchese *et al.* 2011) honeypot projects. (b) Ratio of Windows operating systems that scanned our honeynet.

SSH was implemented in order to further study the brute force attacks against the deployed honeynet in UPM. During the two week period, 32,650 SSH brute force attempts were observed. Attackers poked the SSH port to define the type of SSH service running on the honeynet. Table 3 illustrates the top IP addresses that poked the SSH to get information about running services on it. Most of the SSH connection attempts originated from the US and Russia. If such an operation in determining running services succeeds, the entire system platform is at imminent risk. Therefore, this type of incident must be monitored with high priority.

Table 3: Top IP addresses that poked the SSH to determine the running services.

IP Address	Country	City	Number of scans
128.71.176.225	Russia	Vologda	4,461
74.91.98.48	US	Madison	4,300
114.179.18.37	Japan	Tokyo	2,602
50.166.215.132	US	Beverly	2,268
175.143.235.44	Malaysia	Seri Kembangan	2,013
Too Many	China	----	1,073
219.254.50.8	South Korea	Seoul	444
210.186.218.173	Malaysia	Seri Kembangan	304
175.143.236.22	Malaysia	Seri Kembangan	192
115.187.211.155	Australia	Alexandria	160
84.24.42.60	Netherlands	Kaatsheuvel	155
76.174.131.117	US	Murrieta	152
184.18.151.21	US	Rochester	93
204.210.122.139	US	Honolulu	52
221.155.180.30	South Korea	Seoul	48
210.133.181.1	Japan	Tokyo	19
119.40.112.96	Malaysia	Selangor	10
121.172.8.36	South Korea	Seoul	8
198.143.159.137	US	Chicago	7

5. CONCLUSION

In this paper, a hybrid honeynet, including both low- and high-interaction honeypots, was developed and implemented using virtualisation technology. Both the low- and high-interaction honeypots, consisting of Linux and Windows operating systems respectively, were deployed for a period of two weeks in order to gain a better understanding of the attacks. The observed attacks, and their vulnerabilities were analysed and classified. The network scans were mostly carried out by infected computers on the network. Unsurprisingly, most attacks were carried out by Windows XP computers as Microsoft has suspended new security updates to the platform, while due to regular updates, the number of infected Linux systems were low compared to Windows variants. Russia and US had the highest number of scans on the honeynet, with almost half of the scans from Russia originating from Windows XP computers.

As the honeynet was implemented on a single server rack, it was not possible to extend the complexity of the honeypots as the system could become unstable due to large memory requirements. Future implementations with a more complex honeynet layout and better server setup can yield better understanding of the network probes.

REFERENCES

Abbasi, F.H. & Harris, R.J. (2009). Experiences with a Generation III virtual Honeynet. *2009 Australasian Telecommun. Netw. Appl. Conf. (ATNAC)*, 10-12 November 2009, pp. 1-6.

Albin, E. (2011). *A Comparative Analysis of the Snort and Suricata Intrusion-Detection Systems*, Naval Postgraduate School, Monterey, California.

Awad, J. & Derdmezis, A. (2005). *Implementation of a High Interaction Honeynet Testbed for Educational and Research Purposes*. Available online at: http://www. aitdspace. gr/xmlui/handle/123456789/245 (Last access date: 4 March, 2012).

Bao, J., Ji, C. P., & Gao, M. (2010). Research on network security of defense based on Honeypot. *2010 IEEE Int. Conf. Comput. Application Syst. Model. (ICCASM)*, Vol. 10, pp. V10-299.

Benzel, T., Braden, B., Faber, T., Mirkovic, J., Schwab, S., Sollins, K., & Wroclawski, J. (2009). Current developments in DETER cybersecurity testbed technology. *IEEE Conf. Homeland Secur.: Cybersecur. Appl. Tech. 2009 (CATCH'09)*, pp. 57-70.

Binu, A., & Kumar, G. S. (2011). Virtualization techniques: a methodical review of XEN and KVM. *In* Abraham, A., Mauri, J.L., Buford, B.F., Suzuki, J., & Thampi, S.M. (Eds.) *Advances in Computing and Communications*, Springer, Berlin, pp. 399-410.

Caswell, B., & Beale, J. (2004). *Snort 2.1 Intrusion Detection*. Syngress, Amsterdam.

Cavalca, D., & Goldoni, E. (2010). An open architecture for distributed malware collection and analysis. *In* Huebner, E. & Zanero, S. (Eds.) *Open Source Software for Digital Forensics, Springer*. New York, pp. 101-116.

Mansoori, M., Zakaria, O., & Gani, A. (2012). Improving exposure of intrusion deception system through implementation of hybrid honeypot. *Int. Arab J. Inf. Tech.*, **9**: 436-444.

Gurav, U., & Shaikh, R. (2010). Virtualization: a key feature of cloud computing. *Proc. Int. Conf. Workshop Emerg. Trends Tech.*, pp. 227-229.

Honeynet (2014). *The Honeynet Project*. Available online at: www.honeynet.org (Last access date: 9 September 2014).

Joshi, R. C., & Sardana, A. (2011). *Honeypots: A New Paradigm to Information Security*. Science Publishers, Boca Raton, Florida.

Kaspersky (2014). *Kaspersky Security Bulletin 2013*. Kaspersky, Moscow.

Kaur, J. & Chhabra, G.S. (2012). Design and implementation of Linux based network forensics system using virtual honeynet. *Int. J. Adv. Res. Comput. Eng. Tech.*, **1**: 504-508.

Li, Z., Goyal, A., & Chen, Y. (2008). Honeynet-based botnet scan traffic analysis. *In* Lee, W., Wang, C. & Dagon, D. (Ed.) *Botnet Detection*. Springer, New York, pp. 25-44.

Liu, X., L. Peng, et al. (2011). The dynamic honeypot design and implementation based on Honeyd. In Lin, S. & Huang, X. (Eds.) *Advances in Computer Science, Environment, Ecoinformatics, and Education*. Springer, Berlin, pp. 93-98.

LXC (2014). *LXC – Linux Containers*. Available online at: http://lxc.sourceforge.net (Last access date: 9 September 2014).

Marchese, M., Surlinelli, R., & Zappatore, S. (2011). Monitoring unauthorized internet accesses through a 'honeypot'system. *Int. J. Commun. Syst.*, 24: 75-93.

Musca, C., Mirica, E., & Deaconescu, R. (2013). Detecting and analyzing zero-day attacks using honeypots. *2013 19th Int. Conf. Control Syst. Comp. Sci. (CSCS)*, pp. 543-548.

Nikkhahan, B., Aghdam, A. J., & Sohrabi, S. (2009). E-government security: A honeynet approach. *E-govern.*, **5**: 75-84.

Philippine Honeynet (2014). *Philippine Honeynet*. Available online at: http://www.philippinehoneynet.org (Last access date: 9 September 2014).

Provos, N. (2003). Honeyd-a virtual honeypot daemon. *10th DFN-CERT Workshop*, Hamburg, Germany.

Provos, N., & Holz, T. (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Pearson Education, Upper Saddle River, New Jersey.

Qassrawi, M. T., & Hongli, Z. (2010). Deception methodology in virtual Honeypots. *2nd Int. Conf. Netw. Secur. Wireless Commun. Trusted Comput. (NSWCTC)*, vol. 2, pp. 462-467.

Singh, A. N., & Joshi, R. X. (2011). A honeypot system for efficient capture and analysis of network attack traffic. *2011 Int. Conf. Signal Process., Commun., Comput. Netw. Tech. (ICSCCN)*, pp. 514-519.

Snort (2014). *Snort*. Available online at: http:// http://www.snort.org (Last access date: 9 Sept 2014).

Terzo, O., Ruiu, P., Mossucca, L., Francavilla, A., & Vipiana, F. (2012). Grid Infrastructure for Domain Decomposition Methods in Computational ElectroMagnetics. *In* Maad, S (Ed.) *Grid Computing - Technology and Applications, Widespread Coverage and New Horizons*. Intech, Rijeka, Croatia, pp. 247-266.

Vrable, M., Ma, J., Chen, J., Moore, D., Vandekieft, E., Snoeren, A. C., & Savage, S. (2005). Scalability, fidelity, and containment in the potemkin virtual honeyfarm. *ACM SIGOPS Oper. Syst. Rev.*, **39**: 148-162.

Wang, J., & Zeng, J. (2011). Construction of large-scale honeynet Based on Honeyd. *Procedia Eng.*, **15**: 3260-3264.

Wireshark (2014). *Wireshark*. Available online at: http://www.wireshark.org (Last access date: 9 Sept 2014).

Xavier, M. G., Neves, M. V., Rossi, F. D., Ferreto, T. C., Lange, T., & De Rose, C. A. (2013). Performance evaluation of container-based virtualization for high performance computing environments. 2013 21st Euromicro Int. Conf. Parallel, Distributed and Network-Based Process. (PDP), pp. 233-240.

Yeh, C. H., & Yang, C. H. (2008). Design and implementation of honeypot systems based on open-source software. *IEEE Int. Conf. Int. Secur. Informatics 2008 (ISI 2008)*, pp. 265-266.

ZDNet (2014). *2013 Most Vulnerable Systems & Software: It's Not Just Internet Explorer*. Available online at: http://www.zdnet.com/2013-most-vulnerable-systems-and-software-its-not-just-internet-explorer-7000025924 (Last access date: 9 September 2014).

Zhuge, J., Holz, T., Han, X., Song, C., & Zou, W. (2007). Collecting autonomous spreading malware using high-interaction honeypots. *In* Qing, S., Imai, H. & Wang, G. (Eds.) *Information and Communications Security*. Springer, Berlin, pp. 438-451.

EncryptDecrypt v1.0: A CRYPTOGRAPHIC APPLICATION FOR SENDING MESSAGES VIA COMMERCIAL EMAIL PROVIDERS

Nur Izyan Nabila Komori[1] & Mohamad Ismail Ali[2]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia
[2]Human Resources Management & Support Services Division, Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

Email: nurizyan_nabila@live.com

ABSTRACT

The purpose of this study is to develop an application, named EncryptDecrypt v1.0, which encrypts and decrypts messages to be sent via commercial email providers, such as Yahoo!, Gmail and Outlook.com. In order to ensure that the data to be sent is more secure, the application employs Advanced Encryption Standard (AES) for generating false and true keys, and Triple Data Encryption Standard (3DES) for encrypting and decrypting messages. It is demonstrated that the application is able to encrypt a message and true key to generate a ciphertext and false key respectively, which can then be securely sent to the receiver. The receiver can then decrypt the false key to generate the true key, which is used to decrypt the message.

Keywords: *Cryptology; Triple Data Encryption Standard (3DES); Advanced Encryption Standard (AES); message and ciphertext; false and true keys.*

1. INTRODUCTION

Cryptography is the science of writing in secret code by implementing mathematical and computer sciences. Its strength in securing data has been proven since the World War II era, and now, modern cryptography has been invented for better network security. According to Rivera (2014), some companies failed to keep their data secure due to failure in keeping up with new and emerging threats. This will lead to data leakage and weaken the security strength. Referring to Sarah Palin's hacked email in 2008, it is not difficult to hack an email account by using some important information or keywords (Shea, 2008). Hence, to avoid hackers from attacking email accounts and leaking the private content, it is recommended to have a secret code to hide the actual data. Some of the data encryptions use encryption software that implements mathematical algorithms both to scramble the contents of emails, by reordering the underlying data, and to decipher the encoded version. The algorithms are activated and protected by numerical 'keys' typically containing 10 or more digits (Adam, 2001).

There are many modern cryptographic algorithms proposed by cryptographers to ensure that confidential communication is secure and difficult to be attacked by hackers. Some of these algorithms are Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES). 3DES is a modified algorithm based on the Data Encryption Standard (DES) algorithm, and implements symmetric and fiestel ciphers. The idea is to encrypt the data multiple times using the same algorithm with different keys, which keeps the data safer. There are no practical cryptanalytic attacks on 3DES algorithm, since the cost of key break down is very high, which is estimated to follow an exponential growth, as compared to single DES (Trappe & Washington, 2002). On the other hand, AES is a symmetric block cipher that is flexible and

supports key sizes of 128, 192 and 256 bits in any combination. It has excellent performance in terms of time to produce keys. The performance of AES depends on the key size; if the key size is larger, the performance of AES decreases due to the increased number of rounds (Stallings, 2006).

In a previous study, Mohamad Ismail *et al.* (2012) implemented various algorithms to encrypt messages sent via web-based applications. Users are allowed to choose preferred algorithms to encrypt the data and send the message via the service provider. However, the encryption can happen in the application only, whereby the communication is limited to STRIDE staff's email accounts. Hence, it is difficult if users prefer to encrypt the data and send it through commercial email providers.

The purpose of this study is to develop an application, named EncryptDecrypt v1.0, which encrypts and decrypts messages to be sent via commercial email providers, such as Yahoo!, Gmail and Outlook.com. In order to ensure that the data to be sent is more secure, the application employs AES for generating false and true keys, and 3DES for encrypting and decrypting messages.

2. METHODOLOGY

2.1 Implemented Cryptographic Algorithms in the Application

In this paper, two cryptographic algorithms are used to develop the cryptographic application. The idea is to use 3DES for encrypting and decrypting messages and AES for encrypting and decrypting the key. The rationale in assigning different algorithms for the two tasks is to ensure that the data that will be sent is safe and hard to break. Since conventional email messaging is not very strong in its security, i.e. hackers can open the personal email account, through this method, the key and message can be sent in a secured way. The key sent is encrypted to be a false key, to prevent hackers from decrypting the message easily. In assigning the two algorithms to the two different steps; encryption and decryption of messages, and generation of false and true keys, a comparative study is conducted to determine which algorithm is suitable to be implemented. Table 1 shows the comparison between 3DES and AES.

The idea of this study is to send the encrypted message to the authorised recipient via conventional email. In order to ensure the security of the files sent, the security needs to be further strengthened. Since the strength of encrypted message depends on the key, we have decided to encrypt the key to become a false key to disguise it from hackers. In order to provide higher security to the key, a strong algorithm needs to be implemented. Thus, AES is used for generating false and true keys, while 3DES is used for encrypting and decrypting messages.

2.2 Development of the Application

2.2.1 Encryption of Messages and Generation of False Key

Figure 1 shows the flowchart for the encryption of messages and generation of false key. The user is prompted to compose the message before the encryption step is done. In this application, the user can type the message in alphanumerical method without attaching any files. Next, the user needs to define a password, which will be the key for message encryption. The key should be unique, so as to preserve the security of the message content. Then, the message is encrypted to generate a ciphertext using 3DES, while the key used to encrypt the message is encrypted using AES to generate the false key. Both the ciphertext and false key are saved as text files. The user can then attach the files easily into a conventional email without copying and pasting the content.

Table 1: Comparison between 3DES and AES.
(Adapted from Alanazi *et. al.*, 2010)

Aspect	AES	3DES
Key length	128, 192 and 256 bits	2 keys – 112 bits 3 keys – 168 bits
Cipher type	Symmetric	Symmetric
Block size	128, 192 and 256 bits	64 bits
Cryptanalysis resistance	Strong against differential, truncated differential linear, interpolation and square attacks.	Vulnerable to differential, brute force attacks. Attackers can crack the plaintext using differential cryptanalysis.
Security	Secure	Weakness in exiting DES
Possible keys	2^{128}, 2^{192}, 2^{256}	2^{112},2^{168}
Time required to check all possible keys	AES-128 : approximately 5 x 10^{21} years	3DES-112 : 800 days 3DES-168 : 1200 days

2.2.2 Degeneration of False Key and Decryption of Message

Figure 2 shows the flowchart for the degeneration of false key and decryption of messages. The user will receive the ciphertext and false key file. In the decryption step, the user is prompted to choose whether to open the files received, or open the text box and paste the ciphertext. While opening the files received, user should browse for the files. After completing the browsing step, the application will read the content of the ciphertext. Then, the false key is decrypted using AES. The generated true key is saved in a text file and used to decrypt the ciphertext. If the false key is used directly to decrypt the message, the decryption will fail due to the wrong key being used. The decryption of the message is implemented using 3DES.

2.3 Application Design

The proposed application is developed using the BASIC programming language, using the Microsoft Visual Basic 2010 Express (VB 2010) software. It allows a programmer to design an application conveniently in a fraction of the time that it would normally take to code a program without using Integrated Development Environment. Visual Basic allows programmer to work directly with graphics, as it gives a disciplined approach to write program clearer than unstructured programs, easy to test, debug and modify (Hassan *et al.*, 2006). The coding is built and ran on an Intel Pentium Dual-Core 2.20 GHz processor with Windows 7 Ultimate 64-bit operating system. The compatibility test is also conducted by running the application on an Intel Pentium Core 2 1.83 GHz processor with Windows XP SP2 32-bit operating system.

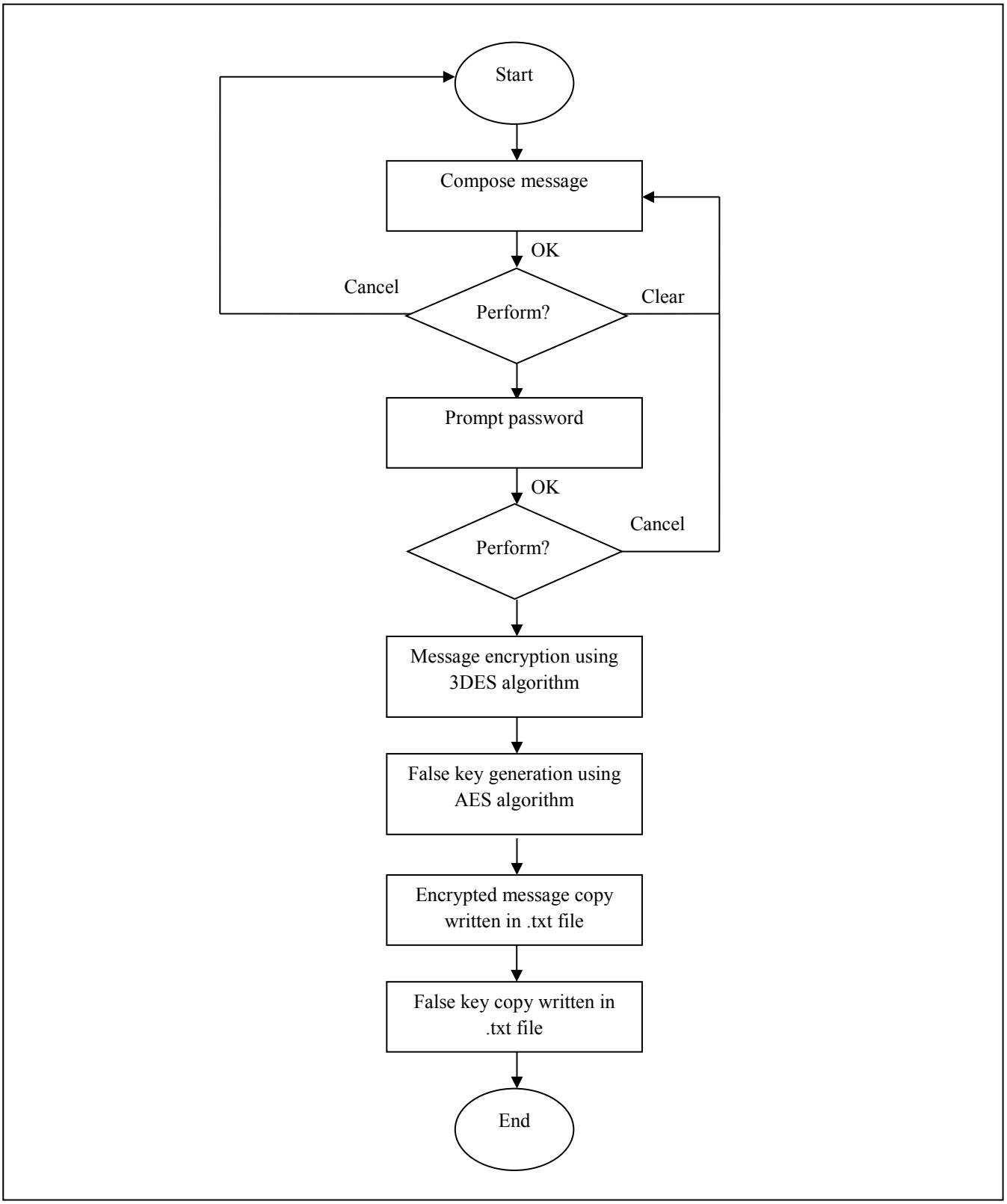
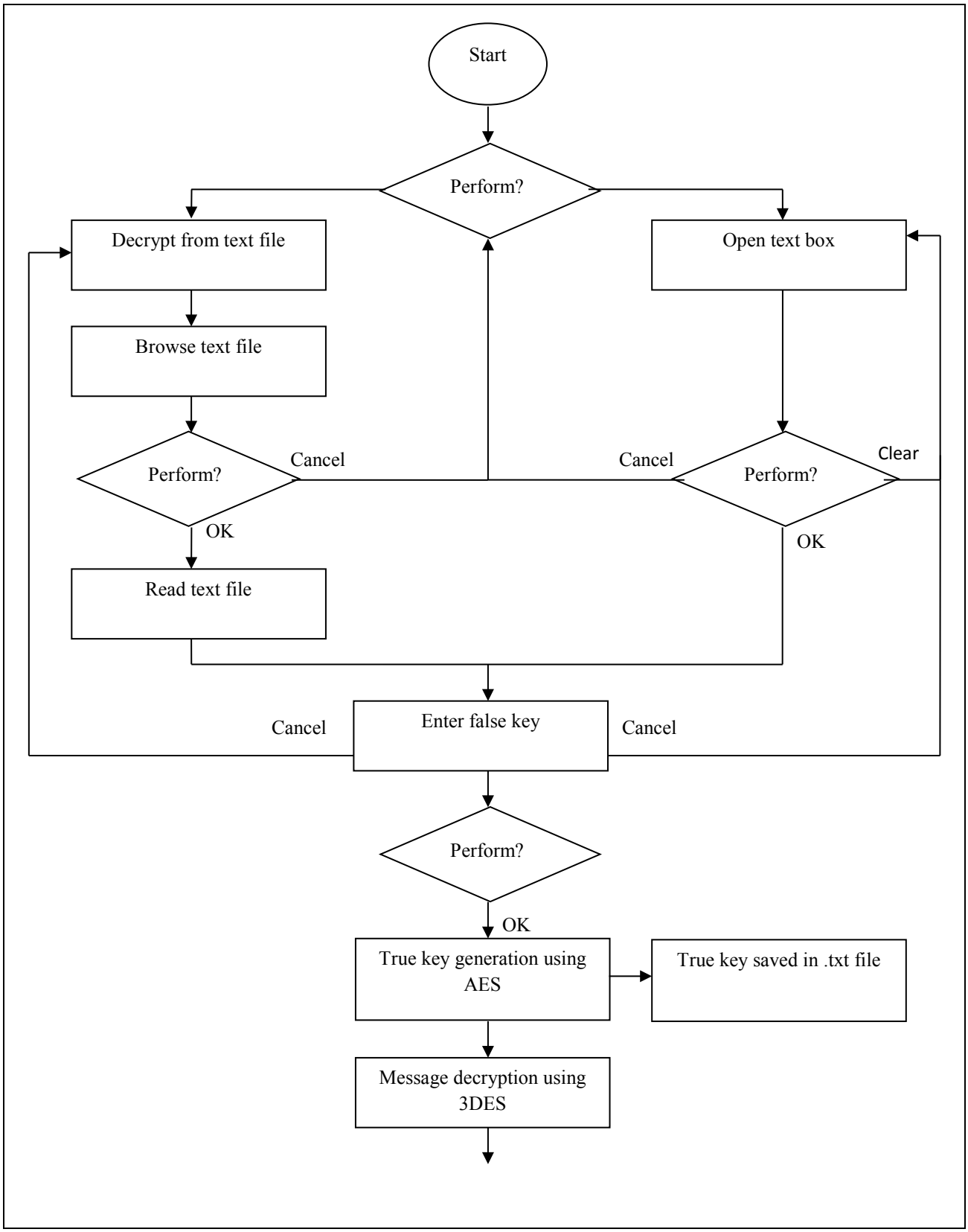


Figure 1: Flowchart for encryption of messages and generation of false key.


Start
Perform?
Decrypt from text file
Open text box
Browse text file
Perform?
Cancel
Cancel
Perform?
Clear
OK
OK
Read text file
Cancel
Enter false key
Cancel
Perform?
OK
True key generation using AES
True key saved in .txt file
Message decryption using 3DES

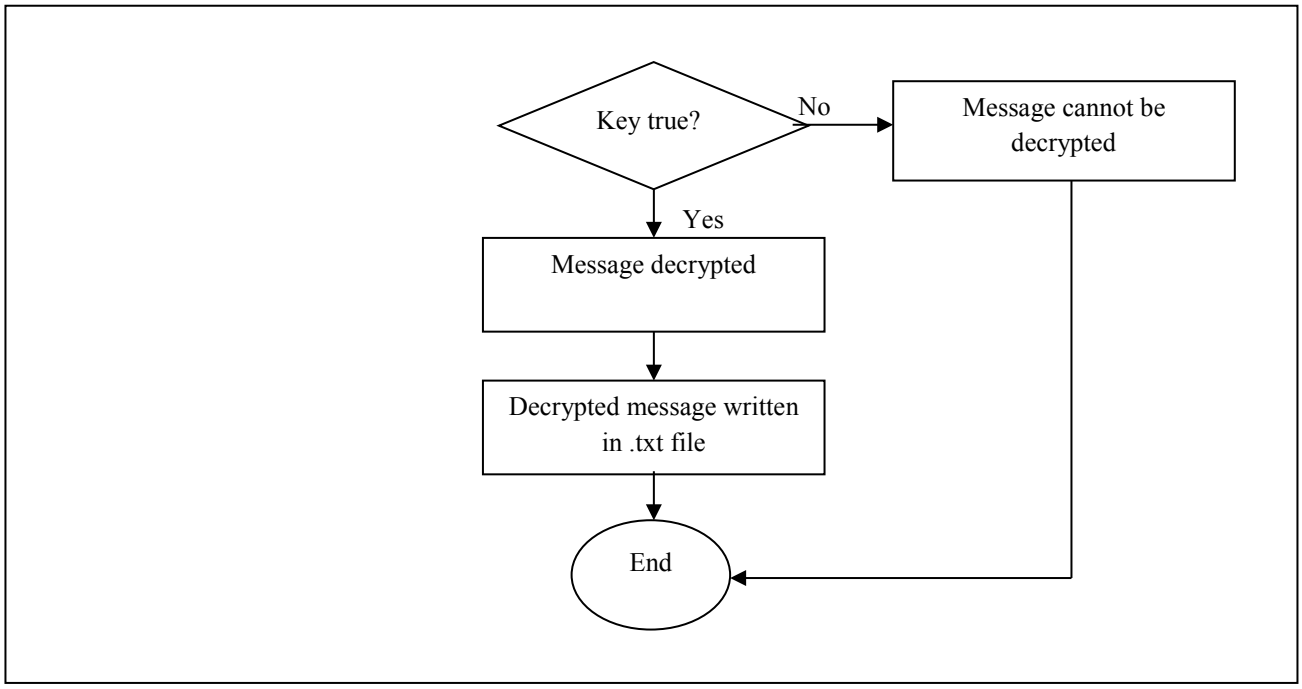


Figure 2: Flowchart for degeneration of false key and decryption of messages.

In designing the application, several packages are used from the Microsoft Developer Network library. The following packages are used in the application:

Imports System.IO (1)
Imports System.Security (2)
Imports System.Security.Cryptography (3)
Imports System.Text (4)

Package 1 is used to allow reading and writing of files and data streams. Package 2 is a general package for security documentation, while Package 3 is one of the documentations served in the *Security* package, which provides cryptographic services. Package 4 is used to enable the encoding classes to be used in the application.

In this application, base classes are also used, which are inherited from the *Cryptography* package. The following base classes are used in building the application:

AesCryptoServiceProvider() (5)
Rfc2898DeriveBytes() (6)
SHA1CryptoServiceProvider() (7)
TripleDESCryptoServiceProvider() (8)

Base class 5 is used to implement AES. It performs symmetric encryption and decryption using Cryptographic Application Programming Interfaces (CAPI). Base class 6 implements password-based key derivation by using a pseudo-random number generator, while base class 7 computes the SHA1 hash value for the input data using the implementation provided by the cryptographic service provider. Then, base class 8 is used to implement 3DES.

3. RESULTS AND DISCUSSION

The EncryptDecrypt v1.0 application is developed with a user-friendly interface that is easy for beginners to understand. The main menu (Figure 3) consists of two functions which are the encryption and decryption steps.

Figure 3: The main menu of the EncryptDecrypt v1.0 application.

Under the encryption function, the user is prompted to compose the message. Figure 4 shows the text box for message composition. In this application, only alphanumeric content is supported. The content of the message is ready to be encrypted when the user clicks the 'OK' button. The 'Cancel' button aborts the encryption function and returns the user to the main menu. The 'Clear' button is used to clear the content of the text box.

The 'OK' button leads the user to the next step. A popup window will appear and prompt the user to enter the true key (user-defined password) (Figure 5). Then, the message is encrypted using the true key and stored in a text file (Figure 6). The true key and ciphertext are stored in a different text file for backup. A false key is then generated, also as a text file (Figure 7). Then, the user can attach the ciphertext and false key files in a single email.

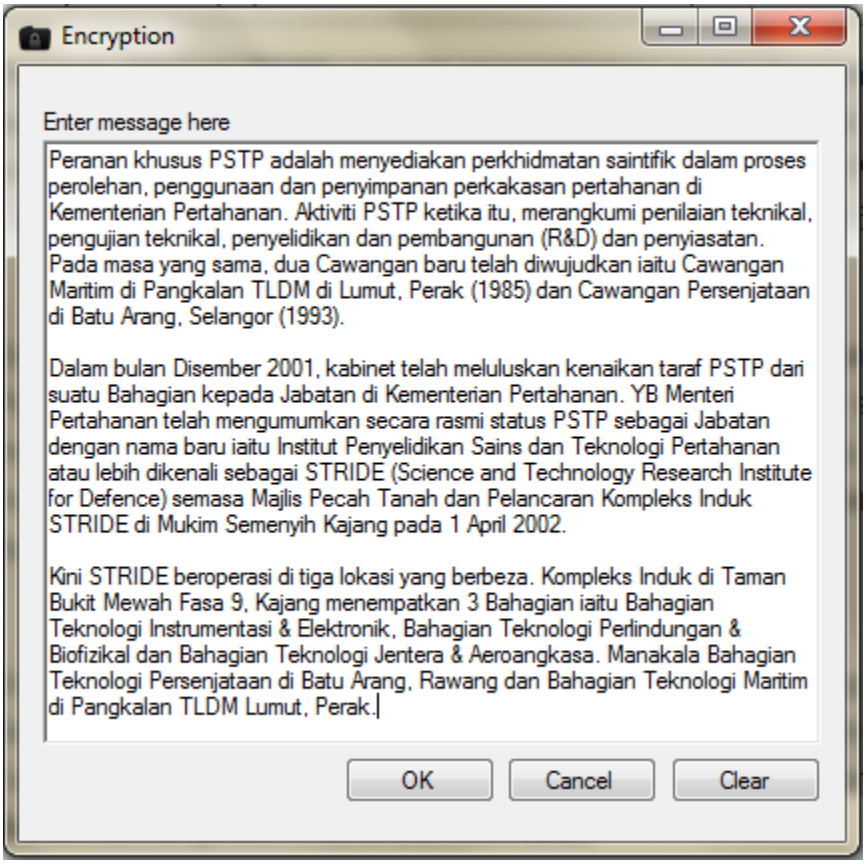


Figure 4: Message composition before encryption

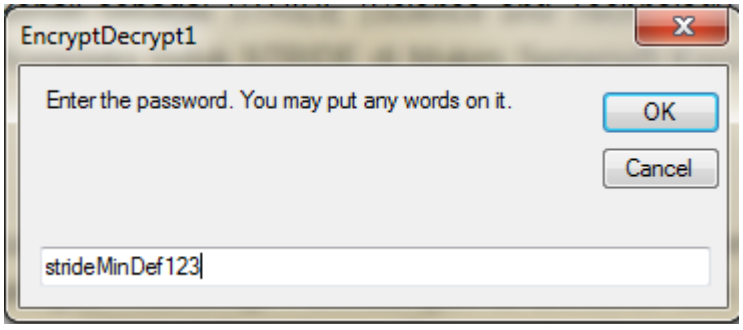


Figure 5: Setting up the true key (user-defined password)

Figure 6: The ciphertext for the message in Figure 4.

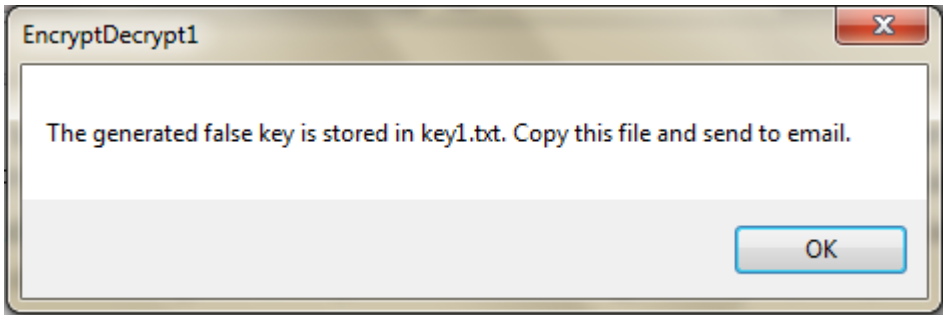


Figure 7: The generated false key information window.

In the decryption function, there are two options for the user to choose; whether to open received files directly or paste the ciphertext into a text box (Figure 8). By opening the files directly, the user needs to browse the files first before decrypting them (Figure 9). Then, the decryption of the false key to true key is implemented.

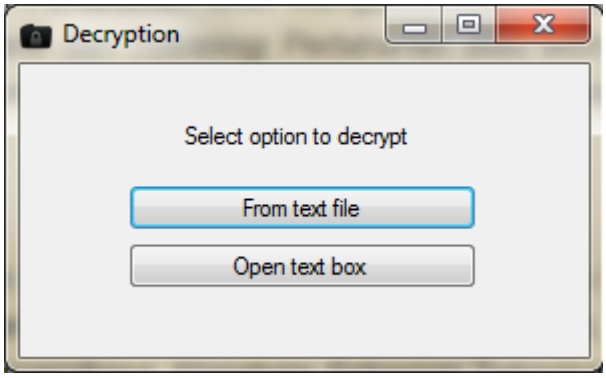


Figure 8: The provided options to decrypt the received files.

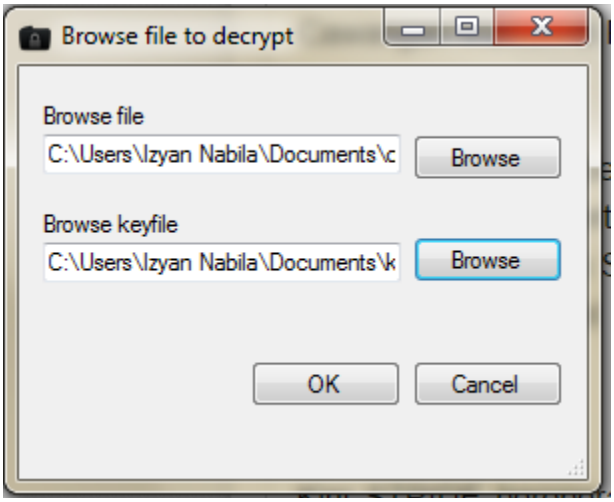


Figure 9: Browsing files to be decrypted.

By opening text box, users are prompted to browse for false key file and pasting the content of ciphertext (Figure 10). Decryption of the false key is implemented by clicking the 'OK' button. The true key is generated and stored in a text file for backup (Figure 11). It is then used to decrypt the message (Figure 12).

The result shows that the decrypted message (Figure 13) is the same as composed message sent by the sender. To handle problems such as entering the wrong true key, an exception handling has been inserted into the coding. If the user enters the wrong true key (Figure 14), the decryption of the message cannot be carried out (Figure 15).

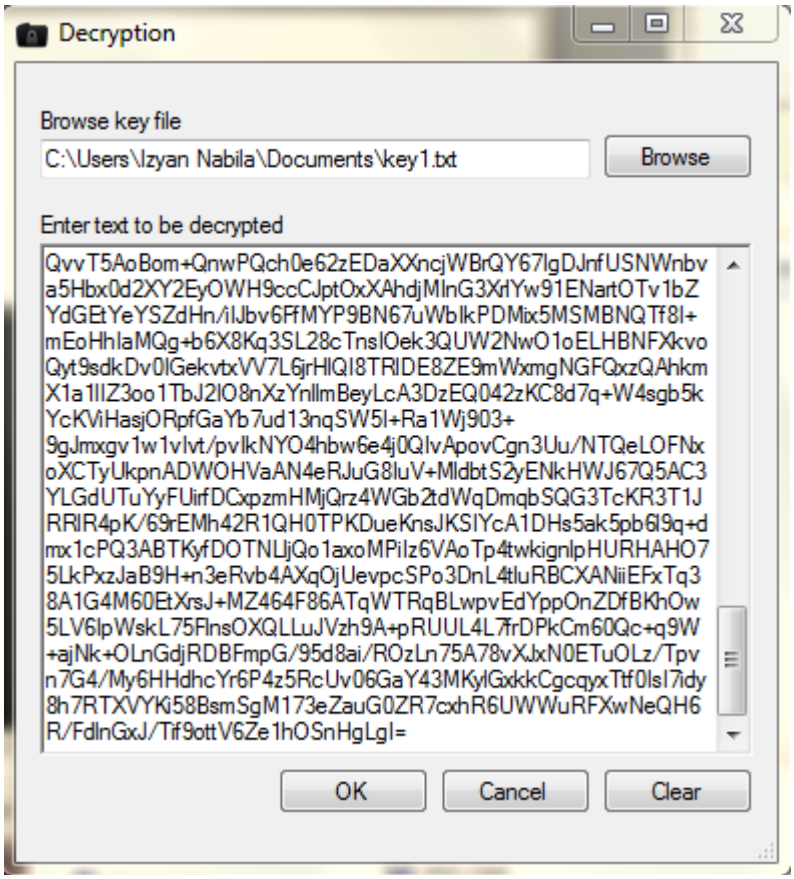


Figure 10: The decryption option by opening the text box.

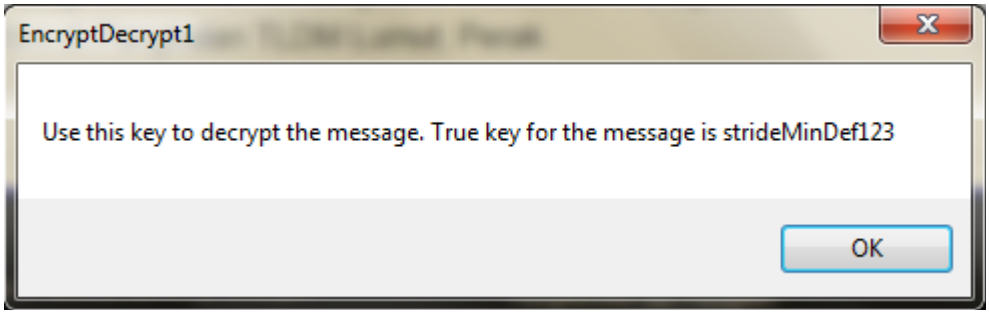


Figure 11: The true key is generated.

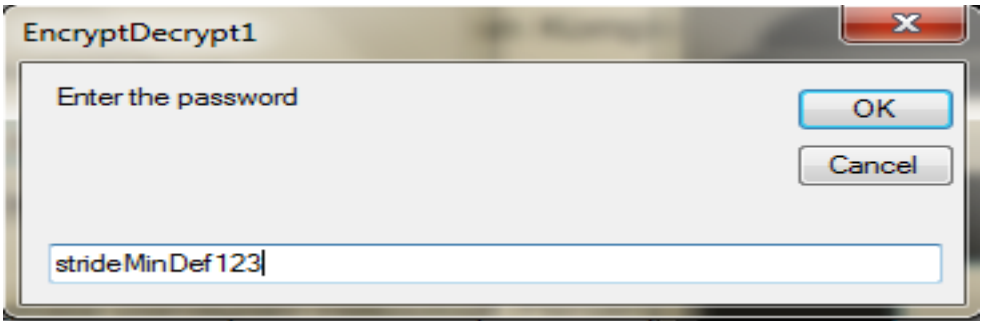


Figure 12: Entering true key to decrypt message.

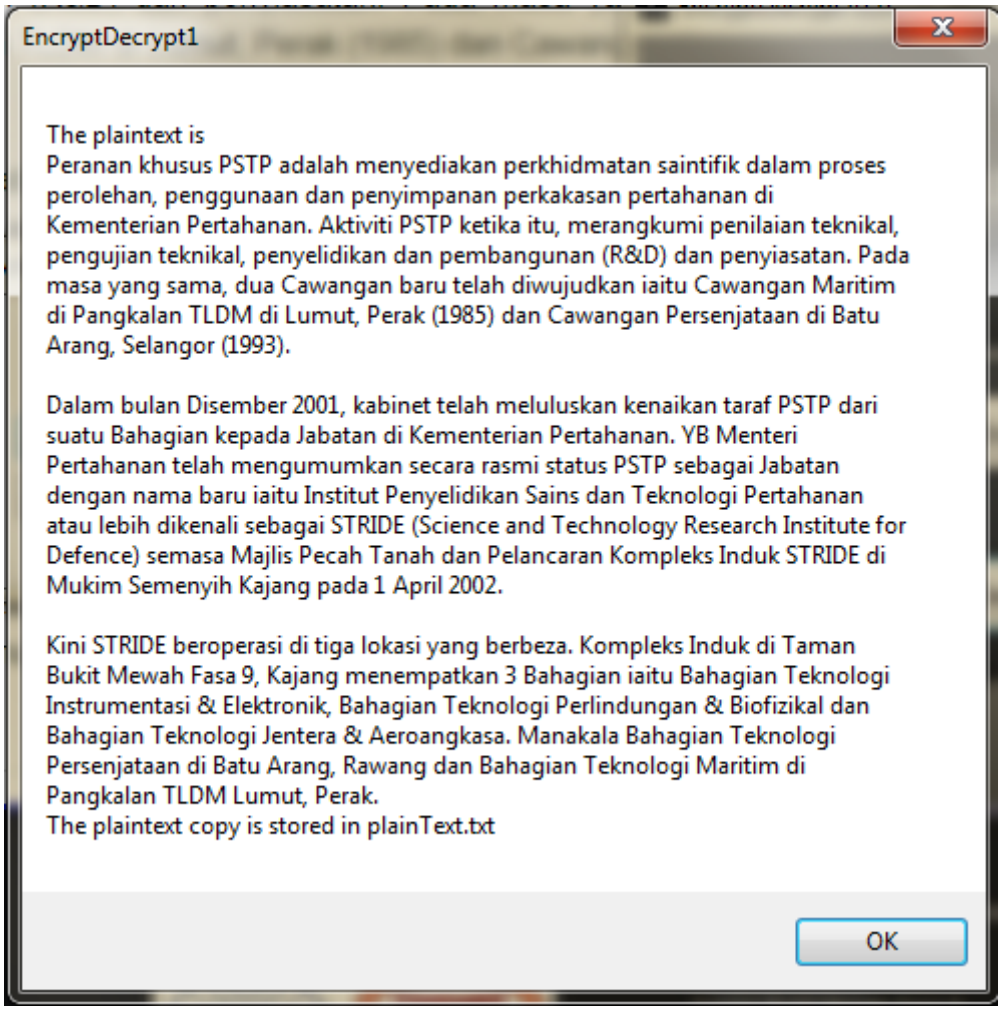


Figure 13: The result after decrypting the ciphertext.

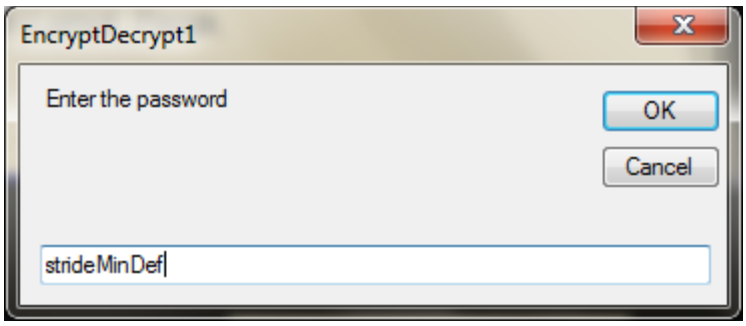


Figure 14: The user entering the wrong true key.

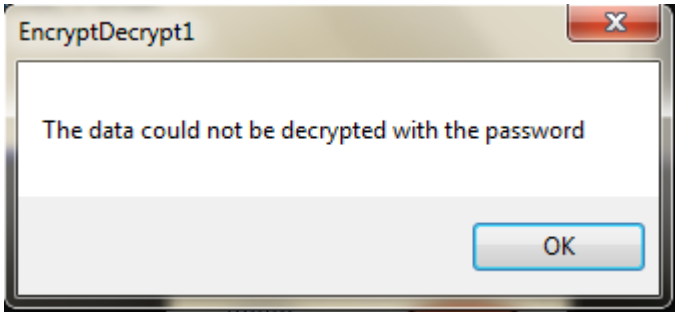


Figure 15: The generated handling exception for message decryption.

4. CONCLUSION

This paper proposed the EncryptDecrypt v1.0 application for sending confidential messages through conventional email. The application implements encryption and decryption of messages by implementing two cryptographic algorithms. In considering the security of a message to be sent, the message is encrypted to generate a ciphertext using 3DES, while the true key is encrypted to generate a false key using AES. The generated ciphertext and false key can then be attached in the email without exposing the true key. The application ran successfully without any error. For further research, it is recommended to enhance the security of the application by hiding the files attached to prevent suspicion of files sent. Steganography may be applied in hiding information as it conceals information from being seen by unauthorised parties.

REFERENCES

Adam, D. (2001). Cryptography on the Front Line. *In* Adam, D., *Nature*. **413**: 766-767.

Alanazi, H.O., B.B. Zaidan, A.A Zaidan, Hamid A. Jalab, M. Shabbir & Y. Al-Nabhani. (2010). New Comparative Study between DES, 3DES and AES within Nine Factors. *J.Comput., **2**,* 152-157.

Hassan, A.B., Abolarin, M.S. & Jimoh, O.H. (2006). The Application of Visual Basic Computer Programming Language to Simulate Numerical Iterations. *Leonardo Journal of Sciences*, **9**, 125-136.

Mohamad Ismail, A., Rozita, M.S., Zariyah, A., Nor Hafizah, M., & Norkamizah M.N. (2012). Development of the Malaysian Armed Forces cryptology capabilities. *Buku Laporan Projek-projek R&D Pertahanan RMK9 &RMK10 Sempena DRC 2011,* 441-450.

Rivera, L. (2014). *Protecting Customer Privacy Through Email Encryption*. Available online at:

http://www.scmagazine.com/protecting-customer-privacy-through-email-encryption/article/337773/ (Last access date: 10 October 2014)

Shea, D. (2008). *Sarah Palin's E-Mail Hacked: How It Was Done*. Available online at: http://www.huffingtonpost.com/2008/09/18/sarah-palins-e-mail-hacke_n_127553.html (Last access date: 13 October 2014)

Stallings, W. (2006). *Cryptography and Network Security, Principles and Practices, 4th Edition*. Pearson Prentice Hall, New Jersey.

Trappe, W. & Washington, L.C. (2002). *Introduction to Cryptography with Coding Theory*. Pearson Prentice Hall, New Jersey.

MULTI-CRITERIA DECISION MAKING (MCDM) FOR TECHNICAL EVALUATION OF TENDERERS: A REVIEW OF METHODS EMPLOYED

Nor Hafizah Mohamed[1*], Hendrik Lamsali[2] & Dinesh Sathyamoorthy[1]
[1]Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[2]Centre for University-Industry Collaboration (CUIC), Universiti Utara Malaysia (UUM), Malaysia

[*]Email: norhafizah.mohamed@stride.gov.my

ABSTRACT

Multi-criteria decision making (MCDM) is an area that is often discussed in operations research (OR). It is able to handle problems involving multiple criteria, and produce meaningful and quality decision making, especially in selecting the best alternative. This paper is aimed at reviewing the applications of MCDM for technical evaluation of tenderers. It identifies the problems that often occur in technical evaluation of tenderers. The MCDM techniques that have been employed to address these problems are then discussed, along with their benefits and limitations. Based on the review conducted, it can be suggested that analytical hierarchy process (AHP) is the most practical MCDM method for technical evaluation of tenderers, as it provides a fair and open process of assessment by taking into consideration the evaluators involved to avoid the issue of bias, and can be carried out with simplicity and transparency. Nonetheless, studies on other MCDM methods should be further explored due to the limitations of AHP.

Keywords: *Technical evaluation of tenderers; multi-criteria decision making (MCDM); group decision making; objectives (goals) and criteria; weighted relative importance.*

1. INTRODUCTION

Procurement systems play an important role in many countries and organisations. Most countries recognise that the nation's development depends on an efficient procurement system, which can ensure the success of projects of state facilities, such as government offices, schools and hospitals, in order to successfully meet the demands of the people. Accountability in the selection of qualified tenderers is important in achieving success in a project. Therefore, in the selection of tenderers, making the right decision, taking into account all of the factors involved, is very important (Tahriri *et al*., 2008; Abu Nemeh, 2012).

The tender procedure is very complex and involves coordination tasks with different priorities and objectives for each item. Cheng & Li (2004) stated that if no system or technique selection is in place to accurately assess the most suitable tenderer, project performance can be affected. Technical evaluation of tenderers is one of the main activities of an organisation in acquisitions, whether in the form of services, supplies or works to facilitate the planning of a project. Bias and inconsistency in judgement are inevitable if the technical evaluation depends on intuition, subjective judgment or emotion. Therefore, a transparent, flexible guidance tool to support the assessment of the tenderers is required to produce a more effective evaluation (Mohemad *et al*., 2010).

Effective technical evaluation of tenderers needs to take into account the diversity of procurement situations that occur in terms of the complexity and importance of all levels.This is associated with problems in the establishment of criteria for the evaluation of potential tenderers, and deciding the final choice among the qualified tenderers. In order to assess the best tenderer, it is important to take into account both quantitative and qualitative factors simultaneously. Managers also need to take into account the various relevant factors in the evaluation process. To this end, based on previous studies,

the assessment of tenderers often involves multi-criteria decision making (MCDM), which is a commonly used tool in OR. This is due to its ability to handle the problem of MCDM and priorities, and to support selection problems that are complex and unstructured. This approach enables decision makers to assess various criteria and compare alternatives to achieve specific goals (Pomerol & Barba-Romero, 2000; Büyüközkan, 2004). The main feature of MCDM is its emphasis on judgment of group decision making, determining the objectives (goals) and criteria, estimating the weighted relative importance, and assessing the contributions of each option for each criteria(DCLG, 2009).

This paper is aimed at reviewing the applications of MCDM for technical evaluation of tenderers. It identifies the problems that often occur in technical evaluation of tenderers. The MCDM techniques that have been employed to address these problems are then discussed, along with their benefits and limitations. This paper is organised as follows: Section 2 describes overview of the MCDM techniques in technical evaluation of tenderers problem. Section 3 describes the challenges faced in technical evaluation of tenders and MCDM techniques employed. Section 4 provides a comparative analysis the MCDM techniques to determine their benefits and limitations. Section 5 suggests the implications of the most practical and prevalent MCDM techniques in technical evaluation of tenderers.

2. OVERVIEW OF THE MCDM TECHNIQUES

2.1 Analytical Hierarchy Process (AHP)

AHP is a technique that has a hierarchy consisting of goals, criteria or factors, sub-criteria and alternatives, comparative judgments, and synthesis of priorities by combining qualitative and quantitative criteria simultaneously. Gabb & Henderson (1996), Yahya & Kingsman (1999), Tam & Tummala (2001) and Shiau *et al.* (2003) found that AHP provides a fair and open process for the technical evaluation of tenderers. The primary advantage of AHP is its simplicity and transparency in developing an interactive selection model to facilitate decision makers in evaluating tenderers (Anagnostopoulos & Vavatsikos, 2006). It is a flexible, easy to use and cost effective method that does not require much time for evaluating and selecting the best tenderers (Palcic & Lalic, 2009). In addition, it is effective and practical for complex tenderer evaluations, whereby judgements are made using pairwise comparisons, which leads to more precise and concise decisions (Padumadasa *&* Rehan, 2009). Hence, the application of AHP technique in evaluation of tenderers provides versatility for various projects, or alternatives and multi-criteria (Kwok, 2011). The importance of each criterion can be seen clearly as it is in the form of a hierarchical structure, while the consistency test reduces bias in making decisions (Aruldoss *et al.*, 2013).

The limitations of AHP are irregularities in rankings and the number of pairwise comparisons needed (Oladapo & Odeyinka, 2006).The decision maker's pairwise comparisons would contain a degree of uncertainty in the preference matrix, which results from doubts expressed by an individual decision maker as to the accuracy of his or her judgments (Wu, 2007). In addition, it is strongly dependent on human judgment as a main element to determine the pairwise comparisons in evaluating tenderers (Aruldoss *et al*., 2013).

2.2 Case-Based Reasoning (CBR)

CBR utilises specific knowledge from previous experiences to create a tenderer evaluation system (Bhattacharya & Karnam, 1997). Its database system can store the performance of past suppliers, which would be used to retrieve and select the tenderers who meet the specifications predefined by the company (Choy & Lee, 2002). However, this method is not capable to enhance the accuracy of the optimal decision in the selection the tenderers. Hence, it must be integrated with other techniques (Alptekin & Büyüközkan, 2011).

2.3 Analytic Network Process (ANP)

ANP replaces the hierarchical structure of AHP with a network structure that depends on the criteria for the purpose of comparison, which is then transferred to the matrix of the weights for all the alternatives. The advantages of this technique are that independence among elements is not required and the prediction is accurate because priorities are improved by feedback. ANP is capable of solving the tenderer problems in which alternatives and criteria have such interactions that cannot be shown in a hierarchy (Sadeghi *et al*., 2012). Among its limitations are that it is time consuming and does not take into account the element of uncertainty in the selection (Aruldoss *et al*., 2013).

2.4 Fuzzy AHP

In this approach, which is an extension to the AHP technique, triangular fuzzy numbers and fuzzy synthesis are used to represent the comparative judgment and determine the priority decisions in accordance with the criteria (Ho *et al*., 2010). Hwang *et al.* (2005) and Mahmoodzadeh *et al.* (2007) used fuzzy AHP in considering the multi-criteria factors related with selecting tenderers. Their findings indicated that this technique is capable of dealing with ambiguity, and managing quantitative and qualitative data simultaneously using fuzzy numbers. However, it needs additional data on optimistic and pessimistic values in human judgements (Rahardjo & Sutapa, 2002).

2.5 Fuzzy Set Theory (FST)

This technique, introduced by Zadeh (1965), uses fuzzy numbers and sets to deal with the ambiguity of human judgments based on rational. This approach is able to evaluate the imprecision involved in the criteria that are subjective or qualitative in the evaluation and selection of tenderers (Sarkar & Mohapatra, 2006; Ho *et al*., 2010). In addition, it can assess the ambiguity of data with the help of mathematical theory and linear programming (Mahmoodzadeh *et al*., 2007). However, it is subjective because it depends on fuzzy numbers, which are not selected on the basis of common agreement, and are complex and difficult to understand (Ulutas *et al*., 2012).

2.6 Data Envelopment Analysis (DEA)

DEA measures the relative importance of the performance of tenderers through the diversity of the inputs and outputs. The advantage of this technique is that it is able to handle data that is not accurate (imprecise data) and identify under-performing units, and provides performance measurement techniques for evaluating the effectiveness of tenderers (decision making units, DMU). Hence, it is widely used in supply chain management (Wu *et al*., 2007). In addition, a variety of inputs and outputs can be applied to this technique, with the relationship between both not being required. Direct comparison of the inputs and outputs can be done even when both are using different units (Aruldoss *et al.*, 2013).

However, the limitation of DEA is that it is not able to measure the efficiency of the tenderers. This can lead to inefficient tenderers getting higher scores than competent tenderers due to the weightage given (Wu *et al*., 2007). This technique is also largely dependent on qualitative criteria and cannot operate if it is not affiliated with any of the MCDM techniques for quantitative criteria (Ho *et al*., 2010; Ulutas *et al*., 2012). Furthermore, its statistical tests cannot be applied for complex problems (Aruldoss *et al*., 2013).

2.7 Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)

TOPSIS is used to determine the list of priorities for the alternatives by calculating the fuzzy positive-ideal (FPIS) and fuzzy negative-ideal (FNIS) solutions simultaneously (Chen, 2006; Mahmoodzadeh *et al*., 2007; Chang, 2010; Nikou & Moschuris 2012). Chen (2006) developed TOPSIS as a conceptual evaluation model in the selection of tenderers. It was found that this technique is able to measure the relative criteria of alternative results in a mathematical form (Mahmoodzadeh *et al*., 2007). In addition, Chang (2010), Yayla *et al.* (2012) and Nikou & Moschuris (2013) formulated TOPSIS models for tenderer evaluation in the semiconductor, garment and defence industries respectively. These studies demonstrated that TOPSIS is able to improve the tenderer evaluation and selection process. However, it is difficult to understand because it consists of many algorithms and needs to be combined with other techniques to obtain results more efficiently (Mahmoodzadeh *et al*., 2007).

3. CHALLENGES IN TECHNICAL EVALUATION OF TENDERERS AND RELEVANT MCDM TECHNIQUES

There are many problems in the evaluation of tenderers, especially in the public sector, such as evaluating on the basis of the lowest bid price, lack of qualified consultants, management pressure to meet budget and time constraints, and lack of experience and knowledge of available decision support systems (Abu Nemeh, 2012). Gabb & Henderson (1996) found that officers in the Australian Defence Organisation (ADO) involved in technical evaluations usually have very tight time constraints, and the requirements to ensure fairness and confidentiality add more pressure to these activities. According to the findings of a case study conducted by Bhattacharya and Karnan (1997), the main problems for acquisitions in India are the lack of data to determine the achievements of tenderers through experience and lack of knowledge among the officers conducting the acquisitions. The selection method applied in evaluating tenderers is case based reasoning (CBR). Choy & Lee (2002) also used CBR in the study on problems in evaluating the performance of tenderers in Hong Kong. China also faces similar problems with other countries because of the wide range of criteria to be taken into account in evaluating tenderers.The approach used to solve this problem is by using analytic network process (ANP) (Wei *et al*., 1997), which is also used in Hong Kong (Cheng & Li, 2004), Korea (Jo & Kim, 2008), Iran (Rafiei & Rabbani, 2009; Sadeghi *et al*., 2012) and India (Vinodh *et al*. 2011).

According to Kwok & Lim (2006), Teo (2010) and Kwok (2011), the evaluation of tenderers in Singapore's Ministry of Defence (MOD) has become more challenging and complex in order to meet the needs of military systems for operations. In addition, MOD also looks into aspects of price, quality, time, abilities of tenderers and, in particular, technical specifications. It uses analytical hierarchy process (AHP) as a decision support tool to complete the tender evaluation process more effectively. AHP is also used in Australia (Gabb & Henderson,1996), Taiwan (Shiau *et al*., 2003; Wang *et al*., 2006), Malaysia (Yahya & Kingsman, 1990; Tam & Tummala, 2001; Manoharan, 2005; Tahriri *et al*., 2008), Lithuania (Banaitienė & Banaitis, 2006), Nigeria (Oladapo & Odeyinka, 2006), Greece (Anagnostopoulos & Vavatsikos, 2006), Slovenia (Palcic & Lalic, 2009), Sri Lanka (Padumadasa & Rehan, 2009), Indonesia (Hendro, 2010) and Saudi Arabia (Abu Nemeh, 2012).

Chen *et al*. (2006) used fuzzy set theory (FST) to handle the problem of uncertainty in the assessment of tenderers to get the ideal solution. India (Sarkar & Mohapatra, 2006) also used the FST to evaluate the performance and capabilities of tenderers based on predetermined criteria. Spain (Garfamy, 2006) used data envelopment analysis (DEA) to avoid the problem of the technical evaluation being conducted in the traditional way, which gives priority to the lowest bidder. United States of America (Seydel, 2006; Wu *et al*., 2007), China (Shen, 2011) and Iran (Toloo & Nalchigar, 2011) also used DEA in solving the problems in the technical evaluation process for selecting the best tenderers.

Taiwan also faced difficulties because of the multi-criteria in the evaluation tenderers, and solved this problem using fuzzy AHP, whereby tenderers are listed in order of importance (Hwang *et al*., 2005). China (Wu, 2007; Chang, 2010) and Greece (Nikou & Moschuris, 2012) used the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) in the evaluation by calculating the weight for each criterion. Evaluation of projects in Iran (Mahmoodzadeh *et al*., 2007) and Turkey (Yayla *et al*., 2012) combined the techniques of fuzzy AHP and TOPSIS.

Table 1 summarises the problems that often occur in the technical evaluation of tenderers and the MCDM techniques employed. For instance, based on table 1, most problems used AHP to solve the problem. Other notable techniques are CBR, ANP, FST, DEA, Fuzzy AHP and TOPSIS.

Table 1: Problems that often occur in the technical evaluation of tenderers and the MCDM techniques employed.

Num.	Authors/ Country	Problems	Technique
1.	Gabb & Henderson (1996) / Australian Defence Organisation (ADO)	Difficulties in the technical evaluation of tenders for various criteria exist for complex acquisitions.	AHP
2.	Bhattacharya & Karnam (1997) / India	No specific method for evaluation of tenderers.	CBR
3.	Wei *et al*. (1997) / China	Issues on criteria to be taken into account for evaluating tenderers.	ANP
4.	Yahya & Kingsman (1999) /Malaysia	Difficult to identify priority rankings of tenderers and allocate the resources of priority needs.	AHP
5.	Tam & Tummala (2001)/ Malaysia	Difficult to evaluate the tenderers of telecommunications systems because of multi-criteria and many tenderers.	AHP
6.	Choy & Lee (2002) / Hong Kong	Difficulties arise in assessing the performance of tenderers.	CBR
7.	Shiau *et al*. (2003) / Taiwan	Evaluation of subcontractor is not effective in selecting the appropriate subcontractor to award the project.	AHP
8.	Cheng & Li (2004) / Hong Kong	Evaluation of tenderers is not effective because the construction management issues involve more complicated decision problems.	ANP
9.	Hwang *et al*. (2005) /Taiwan	Difficulties due to the multiple criteria in the evaluation of tenderers and the need to list the tenderers by priority.	Fuzzy AHP
10.	Manoharan(2005) / Malaysia	Evaluation of tenderers is not effective, causing project delays, cost overruns, non-confirmation on quality, accidents, increase in the number of claims, litigation and contractual issues, and failure to comply to construction specification.	AHP
11.	Chen *et al*. (2006) / Taiwan	Uncertainties in evaluating the tenderers to get the ideal solution.	FST

Num.	Authors/ Country	Problems	Technique
12.	Sarkar & Mohapatra (2006) / India	Difficulties in evaluating the performance and capabilities of the tenderers for various criteria.	FST
13.	Garfamy (2006) / Barcelona, Spain	Tenderer evaluation based on traditional methods, whereby priority is given to the lowest bidder, which makes it hard to ensure the achievement of the tenderer.	DEA
14.	Anagnostopoulos &Vavatsikos (2006) / Greece	Evaluation of tenderers is made based on low prices only.	AHP
15.	Seydel (2006) / US	Significant problems involving limited alternatives and multiple criteria, whereby it is difficult to determine the weights of each criterion in the evaluation of the tenderer.	DEA
16.	Kwok & Lim (2006) / Ministry of Defence, Singapore	Tenderer evaluations for procurements are complex and challenging because of the need to meet military requirements.	AHP
17.	Banaitienė & Banaitis (2006) / Lithuania	Selections are made based on the price of the lowest bid without seeing the commitment, quality and timelines for completion of projects.	AHP
18.	Wang et al. (2006)/Taiwan	Problems in government tenderer selection decisions as it is increasingly complex to select the qualified tenderers to achieve the best value for money and maintaining open and fair competition.	AHP
19.	Oladapo & Odeyinka (2006) / Nigeria	Difficult to select qualified and suitable contractors whilst fostering competitiveness.	AHP
20.	Wu *et al*. (2007) / US	Problems in determining the priority ranking of the tenderers in the evaluation process.	DEA
21.	Wu (2007) / China	Problems in getting competent tenderers in the selection process because their performances influence the benefits of the core enterprise in the supply chain management.	TOPSIS
22.	Mahmoodzadeh *et al*. (2007)/ Iran	Difficulty in getting the best result for tenderer selection when quantitative and qualitative elements exist.	Fuzzy AHPandTOPSIS
23.	Tahriri *et al*. (2008) / Malaysia	Complex problems in supplier selection because it involves qualitative and quantitative multi-criteria to get the optimal supplier combination.	AHP

Num.	Authors/ Country	Problems	Technique
24.	Jo & Kim (2008) / Korea	Supplier selection in the multi-criteria decision-making process dealt with the optimisation of conflicting objectives such as quality, cost and service management.	ANP
25.	Palcic & Lalic (2009) / Slovenia	Difficult to determine the best result of the evaluation of tenderers.	AHP
26.	Rafiei & Rabbani (2009) / Iran	Conflicting criteria and objective function are involved in evaluation of technical projects and vastly employed to cope with the problem.	ANP
27.	Padumadasa & Rehan (2009) / Sri Lanka	Problems in determining the framework to cope with multiple criteria, level of criteria and many tenderers in the evaluation process.	AHP
28.	Chang (2010) / China	Rating of tenderers' equipment has various criteria for semiconductor industries.	TOPSIS
29.	Hendro (2010)/ Indonesia	Problems in determining the priority ranking of the criteria in the selection suppliers.	AHP
30.	Kwok (2011) / Defence Science and Technology Agency (DSTA), Singapore	Diversity in the composition of each project in the tenderer evaluation should meet the needs of military operations.	AHP
31.	Shen (2011) / China	Problems in making strategic decisions in the evaluation of tenderers for food services.	DEA
32.	Toloo & Nalchigar (2011) / Iran	The success of a supply chain is highly dependent on selection of best suppliers.	DEA
33.	Vinodh et al. (2011) / India	Supplier selection encompassing various criteria and sub-criteria need to be taken into account in the supplier selection process.	ANP
34.	Abu Nemeh (2012)/ Saudi Arabia	Selections are made based on low bid price, in addition to problem of lack of qualified consultants, budget pressures, limited time and lack of experience.	AHP
35.	Nikou & Moschuris (2012) / Ministry of Defence,Greece	Difficulty in making the selection of the tenderer for critical defence procurements.	TOPSIS
36.	Yayla *et al*. (2012) / Turkey	Difficulties in evaluating tenderers for the various representations of quantitative and qualitative criteria.	Fuzzy AHP and TOPSIS
37.	Sadeghi *et al.* (2012) / Iran	Supplier evaluation and selection need to consider more than one factor or	ANP

Num.	Authors/ Country	Problems	Technique
		criterion, which may be inconsistent and contradictory in a group of decision makers.	
38.	Gholipour *et al.* (2014) / Iran	Problems in making decision in handling the ambiguous nature of contractor selection.	Fuzzy AHP

4. COMPARATIVE ANALYSIS OF MCDM TECHNIQUES USED FOR TECHNICAL EVALUATION OF TENDERERS

As discussed in the previous section, various MCDM techniques have been used for the technical evaluation of tenderers. This section presents the comparative analysis of the MCDM techniques. Table 2 summarises benefits and limitations of the MCDM techniques employed in the technical evaluation of tenderers**.**

Table 2: Benefits and limitations of MCDM techniques used for technical evaluation of tenderers.

Num.	Technique	Benefits	Limitations
1.	AHP	Fair and open process for the evaluation of tenderers (Shiau *et al*., 2003). Simplicity and transparency (Anagnostopoulos &Vavatsikos, 2006). Realism, capability, flexibility, easy-of-use, timeliness and cost effectiveness (Palcic & Lalic, 2009). Effective and practical for complex tenders, making use of pairwise comparison analysis, which is simple and accurate (Padumadasa & Rehan, 2009). Versatility for a variety of projects or alternatives and criteria (Kwok, 2011). The importance of each criterion can be seen clearly as it is in the form of a hierarchical structure, while the consistency test reduces bias in making decisions (Aruldoss *et al*., 2013).	Irregularities in rankings and the number of pairwise comparisons needed (Oladapo & Odeyinka, 2006). Strongly dependent on human judgment as a main element to determine the pairwise comparisons in evaluating tenderers (Aruldoss *et al*., 2013). Inadequate to handle the inherent uncertainty and imprecision associated with the mapping of the decision maker's perception to exact numbers (Wu, 2007).
2.	CBR	Utilises the specific knowledge of previous experience to create a situation (cases)(Bhattacharya & Karnam,1997)	Not capable to enhance the accuracy of the optimal decision and must be integrated with other techniques. (Alptekin & Büyüközkan, 2011).
3.	ANP	Independence among elements is not required and prediction is accurate because priorities are improved by feedback (Aruldoss *et al*., 2013).	Time consuming and does not take into account the element of uncertainty in the evaluation (Aruldoss *et al*., 2013).

Num.	Technique	Benefits	Limitations
4.	Fuzzy AHP	Capable of dealing with ambiguity, and managing quantitative and qualitative data simultaneously using fuzzy numbers (Hwang *et al*., 2005; Mahmoodzadeh *et al*., 2007).	Needs additional data on optimistic and pessimistic values in human judgement (Rahardjo & Sutapa, 2002).
5.	FST	Fuzzy sets are able to evaluate the imprecision of criteria that are subjective (Sarkar & Mohapatra, 2006; Ho *et al*., 2010). Can assess the ambiguity of data with mathematical theory and linear programming (Mahmoodzadeh *et al*., 2007).	Subjective because it depends on fuzzy numbers, which are not selected on the basis of common agreement, and are complex and difficult to understand (Ulutas *et al*., 2012)
6.	DEA	Is able to handle data that is not accurate (imprecise data) and identify under-performing units, and provides performance measurement techniques for evaluating the effectiveness of tenderers (decision making units, DMU) (Wu *et al.*, 2007). A variety of inputs and outputs can be applied to this technique, with the relationship between both not being required. Direct comparison of the inputs and outputs can be done even when both are using different units (Aruldoss *et al*., 2013).	Not able to measure the efficiency of the tenderers (Wu *et al*., 2007). Cannot operate if it is not affiliated with any of the MCDM techniques for quantitative criteria (Ho *et al*., 2010; Ulutas *et al*., 2012). Its statistical tests cannot be applied for complex problems (Aruldoss *et al*., 2013).
7.	TOPSIS	Able to measure the relative criteria of alternative results in a mathematical form (Mahmoodzadeh *et al*., 2007).	Difficult to understand because it consists of many algorithms and needs to be combined with other techniques to obtain results more efficiently (Mahmoodzadeh *et al*., 2007).

5. IMPLICATIONS AND RECOMMENDATION

Based on the review conducted, it is found that AHP is the most practical and prevalent MCDM technique for technical evaluation of tenderers. It provides a framework to cover multi-criteria, in which the structural problem is assessed in the form of a hierarchy to evaluate the criteria, sub-criteria and alternatives. Moreover, it provides a fair and open process of assessment by taking into consideration the evaluators involved to avoid the issue of bias, and can be carried out with simplicity and transparency. The assessment is made using pairwise comparisons based on the judgement of the decision makers.The importance of each criterion can be seen more clearly and in detail as it is in the form of a hierarchical structure. AHP also provides a consistency ratio to determine the dependability of the decisions made.

AHP depends on the evaluators giving the weight for each criterion. Obviously the evaluators involved must have expertise in the procurement of items rated as only the experts understand the criteria for the procurement specifications. The evaluators must have a level of strategic expertise to determine the importance of all aspects, such as the functionality of equipment or technology expertise. The procurement officer is also an important factor in the evaluation of tenderers,

particularly those involved in the assessment of the tenderer as it requires high expertise and skill on the items tendered in order to facilitate the assessment (Abu Nemeh, 2012).

As AHP procedures relate to individual and group decision making settings, the appropriate approach is to use a lot of evaluators to avoid marginal decisions (Saaty, 1980; Saaty & Vargas, 1994; Büyüközkan, 2004; Ishizaka & Nemery, 2013).Some case studies recommend the use of three to seven evaluators to reduce the bias in assessing comparison pairs (Saaty & Vargas, 1994).

Previous studies have shown that AHP is often used as a tool to perform the evaluation of tenderers to obtain the best decisions more effectively. It is commonly used in the industrial, factory, business, health and education sectors (Kunz, 2010). In addition, a number of countries use AHP to evaluate tenderers for defence procurements, including Australia (Gabb & Henderson, 1996), Hong Kong (Cheng & Li 2004), Singapore (Kwok & Lim., 2006; Koh 2009; Teo, 2010; Kwok, 2011), Taiwan (Shiau *et al*., 2003), Lithuania (Banaitienė & Banaitis, 2006), Greece (Anagnostopoulos,& Vavatsikos, 2006), Slovenia (Palcic & Lalic, 2009), Indonesia (Hendro, 2010) and Saudi Arabia (Abu Nemeh, 2012).

In Malaysia, AHP has been adopted tenderer evaluations. For example, Yahya & Kingsman (1999) implemented this technique, where it is used to identify priority rankings of tenderers and allocate the resources of priority needs. Tam & Tummala (2001) used AHP for the evaluation of tenderers of telecommunications systems. Similarly, Manoharan (2005) presented the AHP model in evaluation of sub-contractors. In addition, Tahriri *et al*. (2008) also applied this technique for the evaluation of tenderers to determine which should be selected to carry out the projects of a steel company.

A significant disadvantage of AHP is its dependence on human judgment. The judgment of the experts must be made in accordance with the procurement's procedures to ensure that no mistakes are made in the selection of tenderers. Furthermore, AHP is complex because of the large number of comparisons that are needed, resulting in difficulties for decision makers in selecting the best tenderers. The selection of criteria is also important in evaluation of tenderers to ensure that the judgment is done accurately and complies with the procurement's requirements. AHP is also unable to handle the inherent uncertainties and imprecisions associated with the mapping of the decision makers' perceptions to exact numbers. Hence, AHP may need to be combined with other methods, such as ANP or DEA, to produce the best decision making method for technical evaluation of tenderers. To this end, studies on other MCDM methods should be further explored due to the limitations of AHP.

6. CONCLUSION

This paper provided a review of MCDM techniques used for technical evaluation of tenderers. It was found that there are numerous problems in tenderer evaluations, with a number of MCDM techniques proposed to solve the problems. Acomparative analysis of these MCDM techniques was then conducted, focusing on their benefits and limitations. While all the techniques are capable of handling multiple quantitative and qualitative factors, the most used approach is AHP, as it provides a fair and open process of assessment by taking into consideration the evaluators involved to avoid the issue of bias, and can be carried out with simplicity and transparency. However, AHP is unable to handle the inherent uncertainties and imprecisions in technical evaluation of tenderers. Hence, other MCDM methods should be explored to address this limitation. This can definitely aid researchers and decision makers in solving tenderer selection problems effectively.

REFERENCES

Abu Nemeh, M.H. (2012). *Multi-Criteria Decision Making Model for the Selection of a Construction Contractor in Saudi Arabia*. Master's dissertation. King Fahd University of Petroleum & Mineral, Dhahran Saudi Arabia.

Alptekin G.I. & Büyüközkan , G. (2011). An integrated case-based reasoning and MCDM system for Web based tourism destination planning. *J. Expert Syst. Appl.*, **38**: 2125-2132.

Anagnostopoulos, K.P. & Vavatsikos, A.P.(2006). An AHP model for construction contractor prequalification.*Int. J. Oper. Res.*, **6**: 333-346.

Aruldoss, M., Lakshmi, T.M. &Venkatesan, V.P. (2013). A survey on multi criteria decision making methods and its applications. *Am. J. Inform. Syst.*, **1**: 31-43.

Banaitienė, N., &Banaitis, A. (2006). Analysis of criteria for contractors' qualification evaluation. Technological and Economic Development of Economy, **8**: 276-282.

Bhattacharya, S. & Karnam, R. (1997). *Knowledge Based Expert System for Optimizing the Decision Making Process in Tender Evaluation*. International Institute of Information Technology, Hyderabad, Gachibowli, India.

Büyüközkan. G. (2004). Multi-criteria decision making for e-marketplace selection. *Internet Res.*, **14**: 139 – 154.

Chang, Y.W. (2010). Multi-attribute decision making on supplier selection in the semiconductor manufacturing company. *Int. Conf. Internet Tech. Appl.*, Department of Aviation Transportation. Management, Aletheia University, Tainan, Taiwan.

Chen, C.T., Lin, C.T. & Huang, S.F. (2006). A fuzzy approach for supplier evaluation and selection in supply chain management. *Int. J. Prod. Econ.,***102**: 289–301.

Cheng, E. W. L., & Li, H. (2004).Contractor selection using the analytic network process. *Constr. Manage. Econ.*, **22**: 1021–1032.

Choy, K.L. & Lee, W.B. (2002). A generic tool for the selection and management of supplier relationships in an outsourced manufacturing environment: The application of case based reasoning. *Logist. Inform. Manage.,* **15**: 235–253.

DCLG (Department for Communities and Local Government) (2009). *Multi-Criteria Analysis : A Manual*. Department for Communities and Local Government (DGLG), London.

Gabb, A. P. & Henderson, D. E. (1996). *Technical and Operational Tender Evaluations for Complex Military Systems*.Department of Defence, Australia.

Garfamy, R.M. (2006). A data envelopment analysis approach based on total cost of ownership for supplier selection. *J.Enterprise Inform. Manage.,* **19**: 662–678.

Gholipour, R., Jandaghi, G. &Rajaei, R. (2014). Contractor selection in MCDM context using fuzzy AHP. *Iran. J. Manage. Stud.*, **7**: 151-173.

Hendro P. (2010). *Sistem Pemilihan Kontraktor Menggunakan Metode AHP*. Politeknik Elektronika Negeri Surabaya, Indonesia.

Ho, W., Xu, X. & Prasanta, K. D. (2010). Multi-criteria decision making approaches for supplier evaluation and selection: A literature review. *Eur. J. Oper. Res.,* **202**:16–24.

Hwang, H., Moon, C., Chuang, C. & Goan, M. (2005). Supplier selection and planning model using AHP. *Int. Symp. Analytic Hierarchy Process 2005*, Honolulu, Hawaii.

Ishizaka, A. & Nemery, P. (2013). *Multi-criteria Decision Analysis: Methods and Software*. John Wiley & Sons, Ltd. UK.

Jo, H. & Kim, T. (2008). *Decision-Making on Multi-Criteria Supplier Selection Using Analytic Network Process*. Department of Industrial & Management Engineering, Kyungsung University, Namgu, Busan, Korea.

Koh, W.L. (2009). *Experience Sharing of AHP Applications.* Defence Management Systems Course (DMSC), Ministry of Defence, Singapore.

Kunz, J. (2010). *The Analytic Hierarchy Process (AHP)*. Eagle City Hall Location.

Kwok, Y.F. (2011). Using Analytic Hierarchy Process for the evaluation of government projects. *Proc. Int. Symp. Analytic Hierarchy Process 2011*, Defence Science and Technology Agency, Singapore.

Kwok, Y.F & Lim, H.S. (2006). Using Analytic Hierarchy Process with operations analysis in project evaluation: 'Unique F-15SG is perfect for Singapore's fighter project'. *Flight Daily*, 21 February 2006.

Mahmoodzadeh, S., Shahrabi, J., Pariazar, M. & Zaeri, M. S. (2007). Project selection by using Fuzzy AHP and TOPSIS technique. *World Acad. Sci. Eng. Technol.*, **6**: 333-338.

Manoharan, R. (2005). *Subcontractor Selection Method Using Analytic Hierarchy Process*. Master's dissertation. Universiti Teknologi Malaysia, Skudai, Johor.

Mohemad, R., Hamdan, A. R., Othman, Z. A. L. I., Maizura, N., & Noor, M. (2010). Decision support systems (DSS) in construction tendering processes. *Int. J. Comput. Sci. Iss.*, **7**: 35-45.

Nikou, C. & Moschuris, S.J. (2012). Final supplier selection system in military critical items. *J. Econ. Bus.*, **62**: 28-46.

Oladapo, A.A. & Odeyinka, H.A. (2006). Tender evaluation methods in construction projects: a comparative case study. *ActaStructilia*, **13** : 106-131.

Padumadasa, E.U. & Rehan, S. (2009). Investigation in to decision support systems and multiple criteria decision making to develop a web based tender management system. *Int. Symp. Analytic Hierarchy Process 2009,* School of Computing, Asia Pasific Institute of Information Technology Colombo, Sri Lanka.

Palcic, I. &Lalic, B.S. (2009).Analytical Hierarchy Process as a tool for selection and evaluating projects. *Int. J. Sim. Model.*, 8: 16-26.

Pomerol, J.C., & Barba-Romero, S. (2000). *Multicriterion Decision in Management: Principles and Practice*. Kluwer Academic Publishers, USA.

Rafiei, H. & Rabbani, M. (2009). Project selection using fuzzy group analytic network process. *World Acad. Sci., Eng. Technol.*, **58**: 457-461.

Rahardjo, J & Sutapa, N. (2002).Aplikasi Fuzzy Analytical Hierarchy Process dalam seleksi karyawan. *Jurnal Teknik Industri,* **4**: 82 – 92.

Saaty, T.L. & Vargas, L.G. (1994). *Decision Making in Economic, Political, Social and Technological Environments with the Analytical Hierarchy Process*.RWS Publication, Pittsburgh.

Saaty, T.L. (1980). *The Analytic Hierarchy Process*. McGraw Hill, New York.

Sarkar, A., Mohapatra, P.K.J.(2006). Evaluation of supplier capability and performance: A method for supply base reduction. *J. Purchasing Supply Manage.,* **12**: 148–163.

Sadeghi, M., Rashidzadeh, M.A. & Soukhakian, M.A. (2012).Using Analytic Network Process in a group decision-making for supplier selection. *Informatica*, **23**: 621–643.

Seydel, J. (2006). Data Envelopment Analysis for decision support. *Ind. Manage Data Syst.*, **106**: 81–95.

Shen. X. (2011). Food service supplier selection based on data envelopment analysis. *Int. Conference Manage. Sci. Ind. Eng. 2011*, Harbin University of Science and Technology, Harbin, China.

Shiau, Y.C., Tsai, T.P., Wang, W.C. & Huang, M.L.(2003). Use questionnaire and AHP techniques to develop subcontractor selection system. *19th Int. Symp. Automat. Robot. Constr.*, National Institute of Standards and Technology, Gaithersburg, Maryland

Toloo, M. & Nalchigar, S. (2011). A new DEA method for supplier selection in presence of both cardinal and ordinal data. *J. Expert Syst. Appl.*, **38**: 14726–14731.

Tahriri, F., Osman, M. R., Ali, A., Yusuff, R. M., & Esfandiary, A. (2008). AHP approach for supplier evaluation and selection in a steel manufacturing company. *J. Ind. Eng. Manage.*, **1**: 54–76.

Tam, M. C. Y. & Tummala, V. M. R. (2001). An application of the AHP in vendor selection of a telecommunications system. *Omega*, **29**: 171-182.

Teo, C.H. (2010). Management of defence & security acquisition projects. *Int. Conf. Defence Secur. 2010*. 20-21 April 2010, Putra World Trade Centre (PWTC), Kuala Lumpur

Ulutas, A., Kiridena, S & Gibson, P. (2012). A novel model to measure supplier performance in the supplier selection process.7th *Int. Congr. Logistic. SCM Syst.*, Faculty of Engineering, University of Wollongong, Australia.

Vinodh, S., Anesh Ramiya, R. & Gautham, S.G.(2011). Application of fuzzy analytic network process for supplier selectionin a manufacturing organisation. *J. Expert Syst Appl.*, **38**:272–280.

Wang, W.K, Wu, W., Chang, W. B. & Huang, H.C. (2006). *A Knowledge-Based Decision Support System for Government Vendor Selection and Bidding*. Department of Accounting, Yuan-Ze University, Taiwan.

Wei, S., Zhang, J. & Li, Z. (1997). A supplier-selecting system using a neural network. *Int. Conf. Intell. Process. Syst.* 1997, **1**: 468 – 471.

Wu, T., Shunk, D., Blackhurst, J. & Appalla, R. (2007). AIDEA: A methodology for supplier evaluation and selection in a supplier-based manufacturing environment. *Int. J. Manuf. Technol. Manage.,***11**: 174–192.

Wu, M. (2007). Topsis-AHP simulation model and its application to supply chainmanagement. *World J. Model. Simul.*, **3** (3): 196-201.

Yahya, S. & Kingsman, B. (1999). Vendor rating for an entrepreneur development programme: A case study using the Analytic Hierarchy Process method. *J. Oper. Res. Society*, **50**: 916-930.

Yayla, A., Yildiz, A. & Ozbek, A.(2012). Fuzzy TOPSIS method in supplier selection and application in the garment industry.*Fibres Text. East. Eur.J.*, **20**(4): 20-23.

Zadeh, L.A. (1965). Fuzzy sets. *Inform. Control.*, **8**: 338-53.