DEFENCE S&T TECHNICAL BULLETIN

VOL. 7 NUM. 2 YEAR 2014 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 1) is expected to be published in April 2015. The due date for submissions is 11 February 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.

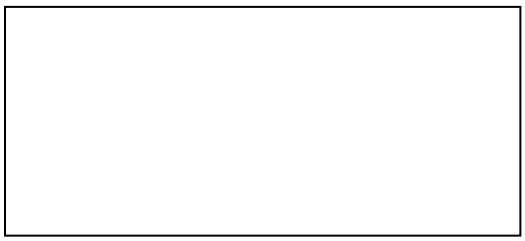


Figure 1: Title of figure.

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.

STUDY ON THE EFFECTS OF ATMOSPHERIC PLASMA SPRAY (APS) PROCESS PARAMETERS ON POROSITIES OF FLY ASH DEPOSITED COATINGS

Mohd Moesli Muhammad[1*], Mahdi Che Isa[1], Azman Jalar[2], Roslinda Shamsudin[2], Syed Rosli Sayd Bakar[3], Mohd Subhi Din Yati[1], Nik Hassanuddin Nik Yussof[1] & Hasril Naim[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
[3]Mechanical & Aerospace Technology Division (BTJA), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

[*]Email: mohdmoesli.muhammad@stride.gov.my

ABSTRACT

This paper focuses on the effect of atmospheric plasma spray (APS) process parameters on the porosities of fly ash deposited coatings. The experiments were constructed using the fractional factorial design approach with four variable parameters, which were powder feed rate, plasma power, and primary and carrier gas pressures. The evaluation of porosities was carried out using image analysis and the Archimedes method. Both analyses showed that the highest porosities content was obtained for sample E1, while the lowest porosities content was obtained for sample E2. The microstructure of the lowest porosities content was influenced by a large fraction of melted region, while the highest porosities content was due to numerous embedded unmelted particles within the splats. The results of analysis of variance (ANOVA) indicated that primary gas pressure, powder feed rate, and the interaction between primary and carrier gas pressures are the most significant factors affecting the porosities of deposited coatings. The interaction effect indicates that lowest porosities content of deposited coatings can be obtained by combining low pressure of carrier gas and high pressure of primary gas.

Keyword: *Fly ash; atmospheric plasma spray (APS); porosities; image analysis; analysis of variance (ANOVA).*

1. INTRODUCTION

Air plasma spray (APS) is a coating deposition technique for ceramic materials. The process involves particles which are injected into a plasma flame by a powder feeder. In the plasma flame, the particles are exposed to high temperature to be melted. The melted particles are accelerated towards a substrate to form splats, which rapidly solidify. The splats overlay on earlier arriving splats to protect the substrate forming deposits or coatings. However, this technique is expensive due to the costs associated with the complex process for spray grade powders (Cao *et al*., 2001). This high cost can be improved by using low grade powders, such as as substitute powders which are cheaper and readily available in industrial waste. For example, many attempts have been carried out to explore the potential of fly ash powders to be used as a feedstock material in APS (Behera & Mishra, 2012; Kutchko & Kim, 2006; Okumus *et al*., 2004). Fly ash is an industrial by-product that is generated in huge quantities during the combustion of coal for energy production in coal-based power plants. Fly ash is a fine powder that is grey in colour, abrasive, mostly alkaline and refractory in nature. Fly ash powders are metal oxides and its major constituents consist of silicon, aluminium, iron and titanium (Acar & Atalay, 2013; Ahmaruzzaman, 2010; Yu *et al.*, 2012).

The final microstructure of APS is affected by multiple spraying parameters, such as primary and carrier gas pressures, powder feed rate, and plasma power. Porosities are defects that are present in the microstructure that can reduce the structure integrity and mechanical properties of deposited coatings. However, the formation of porosities is a desired property due to their ability to act as a thermal barrier coating, which serves to insulate components from large and prolonged heat loads. The evaluation of the porosities can be carried out using many methods, with the most common being image analysis (Portinha *et al*., 2005; Thirumalaikumarasamy *et al*., 2012). In this method, the sample is prepared in a metallographic cross section and the porosities are determined using the images captured using a light microscope or a scanning electron microscope (SEM). This technique is able to distinguish dark pores (voids) and solid structure of the coating materials with sufficient resolution using a post-processing software (Deshpande *et al*., 2004).

The objective of this study is to investigate the effect of APS process parameters on the porosities of deposited coatings using fly ash powders on commercial marine grade mild steel substrates. The experiments were carried out based on fractional factorial design. Four variable parameters were considered simultaneously, which were primary and carrier gas pressures, powder feed rate, and plasma power. The factors that are most significant in contributing to the porosities were analysed using analysis of variance (ANOVA).

2. EXPERIMENTAL METHOD

2.1 Design of Experiments and Sample Preparation

Fly ash collected from the Tenaga Nasional Berhad (TNB) coal-based power plant located in Seri Manjung was used as the feed stock material. The as-received fly ash powder was sieved using a Retsch AS 200 mechanical sieve to obtain particles in the range of 63-100 μm. The cross section of the fly ash powder used is shown in Figure 1, which shows that the particles contain a mixture of spherical and irregular shapes. The structures of the particles are solids, single voids and pores. The chemical composition was analysed using a Bruker SP 4 Pioneer wavelength dispersive X-ray flurosecence (WDXRF) spectrometer. The results of chemical analysis of the fly ash powders are shown in Table 1.

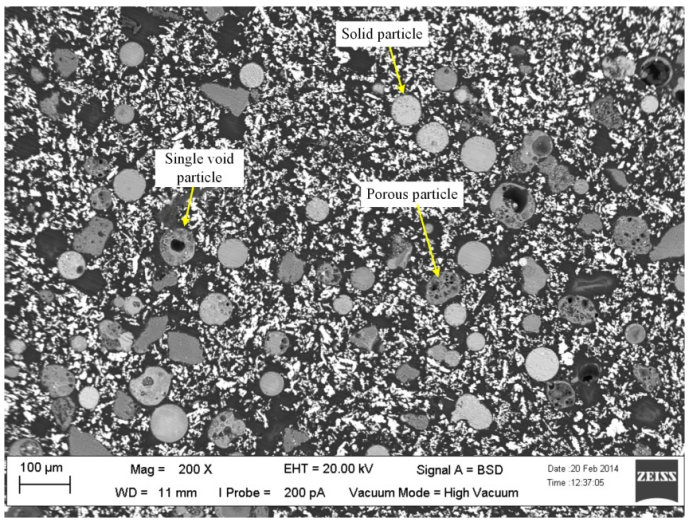


Figure 1: Cross section of the fly ash powders after sieving.

Table 1: Results of chemical analysis of the 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)	Trace
Sulphur (S)	Trace
Phosphorous (P)	Trace
Barium (Ba)	Trace
Manganese (Mn)	Trace

The deposition process was applied on a substrate of A36 mild steel with dimensions of 40 x 30 x 5 mm. Prior to deposition, samples of the substrate surface was grit blasted with aluminium oxide (Al_2O_3), cleaned ultrasonically in ethanol and then dried. The samples were sprayed using a mounted programmable robot type Praxair Surface Technologies SG 100 plasma gun. Four variables of spray parameters were selected for the study, which were primary X_A and carrier X_B gas pressures, powder feed rate X_C, and plasma power X_D. The experiments were designed based on a two-level fractional factorial using the Design Expert, version 8.0.4 software. A total of nine sets of experiments, including one centre point, were run in random order to prevent systematic errors. The spray distance and secondary gas pressure were held constant at 100 mm and 30 psi respectively. Table 2 shows the variables and process parameters for the fly ash plasma spray deposited coatings.

Table 2: Experimental variables and range of values for the process parameters for the experiments conducted.

Parameter	Range
Primary gas pressure X_A (psi)	40, 65, 90
Carrier gas pressure X_B (psi)	30, 37.5, 45
Powder feed rate X_C (rpm)	1, 2, 3
Plasma power X_D (kW)	10, 15, 20
Spray distance (mm)	100
Secondary gas pressure (psi)	30

Figure 2 shows the samples of deposited coatings after the spraying process, which were labelled as E1 to E9 (Table 3). The samples were cut using an Extec Labcut 150 low speed diamond cutter. The samples were then mounted using a Technovit 5000 cold curing resin under vacuum. For the

metallographic procedure, the mounted samples were prepared by grinding using 320-2400 grit silicon carbide abrasive papers finished with polishing of 9 and 3 μm diamond suspension.

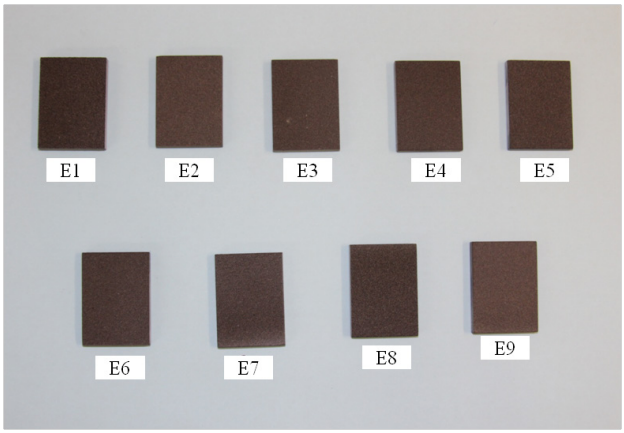


Figure 2: Samples of deposited coatings E1 to E9 obtained after the plasma spray process.

Table 3: Two-level fractional factorial design and process parameters setup for samples E1 to E9.

Sample	X_A (psi)	X_B (psi)	X_C (rpm)	X_D (kW)
E1	40	30	3	10
E2	90	30	1	20
E3	90	45	3	10
E4	90	30	3	10
E5	40	45	1	20
E6	65	37.5	2	15
E7	40	45	3	20
E8	40	45	1	10
E9	90	45	1	10

2.2 Porosities Measurement

Porosities measurement was performed using the images of the polished cross sections of the deposited coatings, which were obtained using a LEO 1430VP SEM in backscattered electron mode at 500x magnification. For each sample, ten micrographs were taken at random locations along the cross section area. Post-processing of the images was carried out using the Image J software. In the first step, the initial image from SEM was cropped, and its brightness and contrast were increased to eliminate interferences and clearly identify the porosities. Then, the image was converted into a binary image using a suitable threshold to extract the porosities from the background. These steps were accomplished through measurement of the area fraction of the porosities in the image using the measurement analysis toolbox in Image J.

As a reference method, the Archimedes method was used to estimate of the deposit porosities through immersion of coating samples in water (Wu *et al.*, 2009). The samples were prepared by forming a rectangular part (deposit + substrates) with dimensions of 10 x 10 mm. The measurement of specific gravity was carried out using a MD-300S Alfa Mirage electronic densimeter. The value obtained in g/cm^3 represents the density of the deposited coatings. This method was selected as the area measured was greater as compared to the image analysis method.

3. RESULTS & DISCUSSION

3.1 Porosities Content

Figure 3 shows the results of porosities obtained using image analysis and the Archimedes method. The bulk volume of the deposited coatings was determined using the Archimedes method, which was complemented with the image analysis results. This is as image analysis can result in high values of porosities due to the metallographic preparation enlarging fine cracks that get counted during analysis (Ondrej *et al.*, 2012). In comparison, for the Archimedes method, the analysis was carried out based on the value of specific gravity, which represents the density of the deposited coatings. The lowest density represents the highest porosities within the structure, while the highest density represents the lowest porosities presence. On the other hand, using image analysis, the results are directly related to the porosities content of the deposited coatings.

Figure 3(a) shows the values of specific gravity for samples E1 to E9. It can be observed that the specific gravity obtained for all the deposited coatings were in the range of 7.0 to 7.7 g/cm^3. These values are lower than 7.89 g/cm^3, indicating that the deposited coatings are less dense than mild steel substrate (Forghani *et al.*, 2012). The highest density (7.75 g/cm^3) was obtained for sample E2, whereas the lowest density (7.05 g/cm^3) was obtained for sample E1.

For the results of the image analysis, as shown in Figure 3(b), the range of porosities content of the deposited coatings was between 9 to 19%. The highest porosities content (18.8%) was obtained for sample E1, while the lowest porosities content (9.56%) was obtained for sample E2.

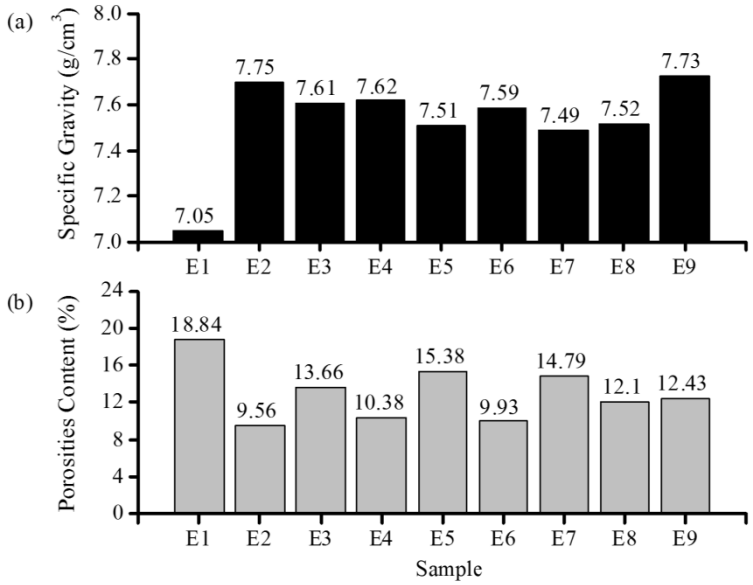


Figure 3: Results of porosities obtained using: (a) the Archimedes method (b) Image analysis.

Both analyses show similar results for the highest and lowest porosities content, which were for samples E1 and E2 respectively. Figure 4 shows the cross section of fly ash deposited coatings for the lowest and highest porosities content. The lowest porosity content was obtained due to a large fraction of melted region within the microstructure. This is due to the particles being completely melted during the spraying process. The melted droplets formed flattened splats and distributed properly on the substrate surface (Figure 4(a)). On the other hand, for the highest porosities content, the impacts of incomplete melted particles produced malformed splats, resulting in numerous unmelted particles embedded within the splats (Figure 4(b)). The splats did not expand well and produced less contact between them, and thus, gaps were created, which are called pores.

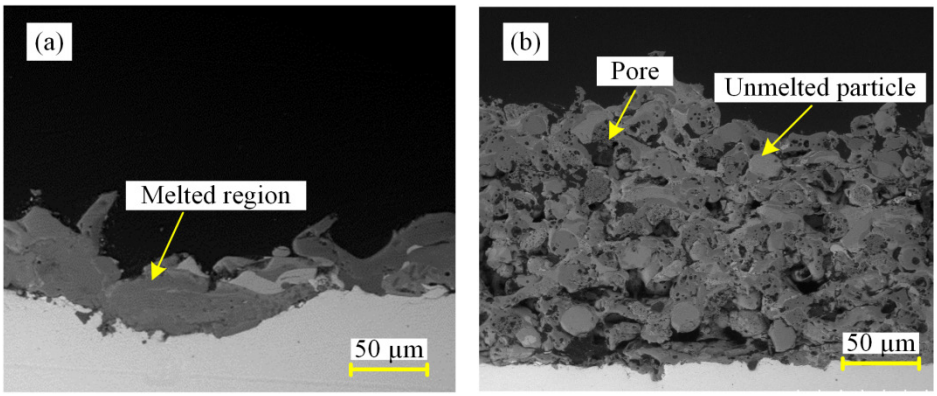


Figure 4: Cross section images of fly ash deposited coatings for the (a) lowest and (b) highest porosities content.

3.2 Effects of Process Parameters on Porosities

Analysis of variance (ANOVA) was performed on the image analysis results using probability of error (*p*-value) less than 0.05, which corresponds to 95% confidence level. The results of the analysis (Table 2) indicates that the porosities of the deposited coatings are affected by three factors, which are X_A (primary gas pressure), X_C (powder feed rate) and X_{AB} (interaction between primary and carrier gas pressures). The regression equation obtained in terms of the coded parameters is as follows:

$$Y = 13.48 - 1.97X_A + 0.94X_C + 1.84X_{AB} \quad (1)$$

Table 4: Results of ANOVA for porosities of the deposited coatings.

Parameter	Coefficient	*p*-value
Porosities Y		0.0112
b_0	13.48	
X_A	-1.97	0.0073
X_C	0.94	0.0737
X_{AB}	1.84	0.0117

*b_0: Mean value of the porosities for all experiments.

This regression equation demonstrates that the two main parameters and an interaction between two parameters have significant effect on the porosities of the deposited coatings. The equation also shows that increasing primary gas pressure has a negative effect on the porosities of deposited coatings, whereas increasing feed rate has a positive effect. However, the presence of interaction among the two parameters in this equation indicates the importance of interaction between parameters rather than just individual parameters (Montgomery, 2009). The interaction is a form of curvature in the underlying response surface model for the experiment, which results in a twist the plane of response. By examining the response results, the effect of factor X_A depends on the the level of factor X_B. Optimisation is achieved when factor X_A is applied at a certain level of factor X_B. Figure 5 illustrates the effect of the interaction between primary and carrier gas pressures on the porosities. The plot indicates that in order to obtain the lowest porosities content, high pressure of primary gas should be combined with the low pressure of carrier gas.

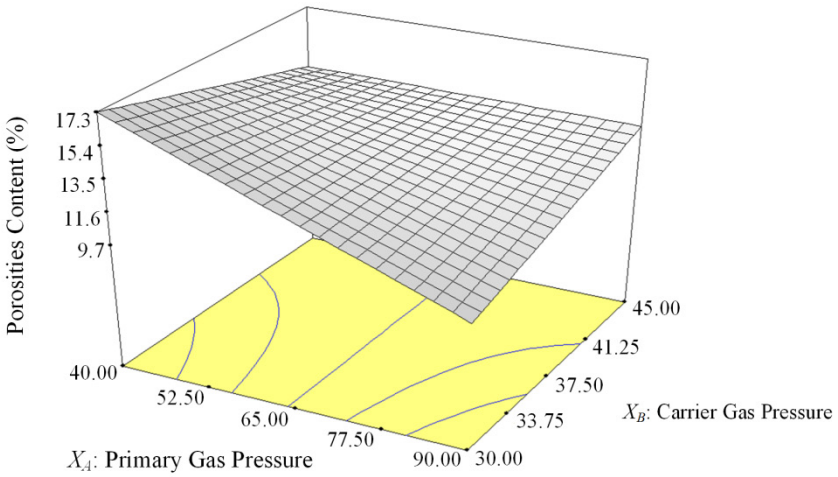


Figure 3: Effect of interaction between primary and carrier gas pressures on porosities of deposited coatings.

The main function of carrier gas pressure in APS is to transmit the powders from the feedstock to the plasma flame through the injector. Therefore, when low pressure of carrier gas is applied, the flow of the particles into the plasma flame is in a steady state. This means that the low pressure does not create any vortex or turbulent flow inside the pipe during the particles' travel to the injector (Ping & Chen, 2001; Xiong *et al*., 2004). At this working pressure, the pattern of plasma flame is retained due to no additional momentum or high velocity gas being induced by the carrier gas pressure. High pressure of primary gas increases the area of plasma formation in terms of width and length of the flame. Consequently, the particles that have been injected will be exposed to high temperature starting from when they enter into the flame and during travelling to the substrate. The kinetic energy of the particles increases and this improves the wetting between the droplets and substrate during collision. Moreover, the high impact of the particles reduces the air or gas trapped within the structure. This phenomenon is due to the effect of flattened splats, which compress on each other during impact on the substrate surface.

4. CONCLUSION

In this study, the porosities of fly ash deposited coatings using APS was determined using image analysis and the Archimedes method. For the image analysis method, the highest porosities content of the deposited coatings was obtained by sample E1, while the lowest was obtained by sample E2. The ANOVA analysis showed that the most significant effects on the porosity were primary gas pressure, powder feed rate and the interaction between primary and carrier gas pressures. The interaction effect indicates that lowest porosities content of the deposited coatings can be obtained by combining low pressure of carrier gas and high pressure of primary gas.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the research funds from DPP-2013-035, FRGS-2-2013-SG06-UKM-02-6 and the Science and Technology Research Institute for Defence (STRIDE). The first author would like to thank the Ministry of Defence for granting him with a study leave to conduct this research.

REFERENCES

Acar, I. & Atalay M. U. (2013). Characterization of Sintered class F Fly Ashes. *Fuel*, **106**: 195-203.

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

Behera A. & Mishra S.C. (2012). Prediction and Analysis of Deposition Effeciency of Plasma Spray Coating Using Artificial Intelligent Method. *Open J. Compos. Mater*., **2**:54-60.

Cao, X. Q., Vassen, R., Schwartz, S., Jungen, W., Tietz, F. & Stöever, D. (2000). Spray-Drying of Ceramics for Plasma-Spray Coating. *J. Eur. Ceram. Soc*., **20**: 2433–2439.

Deshpande, S., Kulkarni, A., Sampath, S. & Herman, H. (2004). Application of image analysis for characterization of porosity in thermal spray coatings and correlation with small angle neutron scattering. *Surf. Coat. Technol.*, **187**:6-16.

Forghani, S.M., Ghazali, M.J., Muchtar, A., Daud, A.R., Yusoff, N.H.N. & Azhari, C.H. (2012). Effects of plasma spray parameters on TiO2-coated mild steel using design of experiment (DoE) approach. *Ceram. Int*., **39**:1-7.

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

Montgomery D. C (2009). *Design and Analysis of Experiments*. John Wiley and Son, Arizona.

Ondrej, K., Petr, H. & Siegl J. (2012). The effect of intersplat porosity on properties of W deposits. *21st Int. Conf. Metal. Mater*., 23-25 May, Brno, Czech Republic.

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

Ping H. L. & Chen X. (2001). Three-dimensional simulation of a plasma jet with transverse particle and carrier gas injection. *Thin Solid Film,* **390**: 175-180.

Portinha, A., Teixeira, V., Carneiro, J., Martins, J., Costa, M.F., Vassen R. & Stoever D. (2005). Characterisation of thermal barrier coatings with a gradient in porosity. *Surf. Coat. Technol.,* **195**: 245-251.

Thirumalaikumarasamy, D., Shanmugam, K. & Balasubramanian, V. (2012). influences of atmospheric plasma spraying parameters on the porosity level of alumina coating on AZ31B magnesium alloy using response surface methodology. *Prog. Nat. Sci. Mater. Int.*, **22**: 468-479.

Wu, C., Ramaswamy, Y., Liu, X., Wang, G. & Zreiqat, H. (2009). Plasma-sprayed $CaTiSiO_5$ ceramic coating on Ti-6Al-4V with excellent bonding strength, stability and cellular bioactivity. *J. R. Soc. Interface*, **6**: 159-168.

Xiong, H.B., Zheng, L.L., Sampath, S., Richard, L.W. & Fincke, J. R. (2004). Three-dimensional simulation of plasma spray: effects of carrier gas flow and particle injection on plasma jet and entrained particle behaviour. *Int. J. Heat Mass Transf*., **47**: 5189-5200.

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 APPROACH FOR PROTECTING CARBON STEEL USING BENZYL DIMETHYL (2-HYDROXYETHYL) AMMONIUM CHLORIDE

Mohd Nazri Idris[1, 2, *], Abdul Razak Daud[1] & Norinsan Kamil Othman[2]

[1]School of Applied Physics, Faculty of Science and Technology, Universiti Kebangsaan Malaysia (UKM), Malaysia
[2]School of Materials and Mineral Resources Engineering, Universiti Sains Malaysia (USM), Malaysia

[*]Email: nazriselama@gmail.com

ABSTRACT

Application of inhibitors to minimize corrosion menace on carbon steel is one of the common practices. Thus, it is important to ensure their performance is adequate to protect the undergoing carbon steel degradation due to corrosion. This paper reports the performance of benzyl dimethyl(2-hydroxyethyl) ammonium chloride (BDC) as corrosion inhibitor for carbon steel which has been investigated by potentiodynamic polarization technique in 1M acetic acid at various concentrations and temperatures. In order to evaluate BDC efficiency, thermodynamics analysis was done and adsorption mechanism had been studied. Potentiodynamic polarization analysis confirmed that BDC reacted as a mix type inhibitor and inhibited the carbon steel on both anodic and cathodic sides. Tafel extrapolated plot revealed that corrosion current density decreased with the increasing of BDC concentration, whereas the corrosion rate of carbon steel increased with the increase in temperature. The inhibition efficiency achieved was up to 90%. Thermodynamic analysis indicated that dissolution of ions could be suppressed as a consequent of adsorption process by BDC molecules on the carbon steel surface. The adsorption mechanism was seen to pursue both physisorption and chemisorptions processes, as it was proven to follow with Langmuir adsorption isotherm. This result was supported by morphological analysis on the carbon steel surface. This study suggests that BDC is a good inhibitor for preventing carbon steel from endures corrosion process in acetic acid medium.

Keyword: *Carbon steel; corrosion inhibitor; inhibition efficiency; adsorption.*

1. INTRODUCTION

Carbon steel has been commercially applied in various industries. In petroleum industries, carbon steel was used as storage tanks and transporting pipeline system for petroleum products. Despite of its high properties performance, carbon steel is easily being corroded either naturally or through any corrosive media, which is directly contacting at its active surface. The used of protective coating, cathodic protection techniques, and adequate corrosion monitoring and inspection are among the best techniques which can be used to protect the external part (Popoola *et al.*, 2013). At the internal part, the most practical method for preventing carbon steel from actively reacts with existing corrosive media such as CO_2, H_2S and organic acid is corrosion inhibitor.

A lot of organic and inorganic compounds have been extensively studied as corrosion inhibitor especially compounds, which are containing heteroatom like N, S, O and P (Mert *et al.*, 2011; Obot & Obi-Egbedi, 2011; Zhang *et al.*, 2011). These atoms possess higher electronegativity than other organic elements and capable of adsorbing onto the steel surface to form a barrier for dissolution process from taking place. Moreover, with the hold of aromatic ring and multiple bonds in an organic compound bear additional pi electron in that inhibitor to be actively contributing with bare steel surface. Existing of unpaired electrons in inhibitor compounds will also increases the inhibitor efficiency as a consequence of sharing activities among these electrons and d-orbital on Fe atom. On top of that, several studies of new potential inhibitor from different functional groups have been

chemically synthesized and formulated (Behpour *et al.*, 2010; Popova *et al.*, 2011; Belfilali *et al.*, 2012). Different types of drugs (Gece, 2011; Singh *et al.*, 2012) have also been explored as well as extraction product from natural plants (Raja & Sethuraman, 2008; Yahya *et al.*, 2013; Mohamad *et al.*, 2014).

In order to evaluate the inhibitor efficiency, several techniques can be implied. Electrochemical method such as potentiodynamic polarization and electrochemical impedance spectroscopy are the most common procedure done. These techniques can be used to determine the kinetic and corrosion behavior of studied metallic compounds based on electrochemical data. Meanwhile, the performance of studied inhibitor can be evaluated. In this study, potentiodynamic polarization technique has been performed to investigate the efficiency of BDC as a corrosion inhibitor for carbon steel used in pipeline system. The performance of this inhibitor in organic acid has rarely been explored. The focus of present study is to identify BDC efficiency as a function of its concentration and temperature in 1 M acetic acid.

2. MATERIALS AND METHODS

Carbon steel used in this study is a standard API5L grade. Analysis of X-ray florescence, model Rigaku RIX3000 confirmed that present carbon steel contained chemical composition (wt%); 0.258 C, 0.466 Mn, 0.427 Si, 0.013 P, 0.015 Ni, 0.019 Cu, 0.132 Al and balance Fe. This steel was mechanically cut and embedded in epoxy resin and the exposed surface area was 0.43 cm^2. The samples have been ground with different grade of silicon carbide paper up to 1200 grade. For each polishing steps, the sample was cleaned with distilled water and rinsed with acetone. BDC was purchased from Sigma Aldrich Co. Ltd and different concentration from 2.5 to 15.0 mM in 1 M acetic acid solution has been prepared.

Potentiodynamic polarization study was carried out by a potensiostat model K47 Gamry framework. The test was conducted in a conventional three electrodes. Platinum rod and saturated calomel electrode (SCE) were used as auxiliary and reference electrode, respectively. Potentiodynamic polarization test was performed in 1 M acetic acid in the absence and presence of 2.5 to 15.0 mM BDC at 25 to 70 $^{\circ}$C. All tests were started after 15 minutes immersion and the polarization curve was recorded from -250 mV to +250 mV of open circuit potential value with the scan rate of 1 mV/s. The morphology of carbon steel was analyzed by scanning electron microscope model Hitachi TM3000.

3. RESULTS AND DISCUSSION

Potentiodynamic polarization method was used to characterize the corrosion behavior and the inhibitor efficiency as a function of its concentration and temperature. Figure 1 represents some of the potentiodynamic polarization analyses on carbon steel surface in 1 M acetic acid, which containing different BDC concentrations at different temperature. Electrochemical parameters such as corrosion potential (E_c), corrosion current density (I_c), anodic Tafel slope (β_a) and cathodic Tafel slope (β_c) were calculated by Tafel extrapolating plot and elucidates in Table 1.

As shown in Figure 1 and calculated values of cathodic Tafel slopes in Table 1 of all BDC concentrations showed no significant changes at all temperatures studied. This result indicated that the mechanism of hydrogen evaluation arises from H^+ reduction process is remaining unchanged. Besides, the changes in values of measured anodic Tafel slopes on most presence BDC concentration probably was attributable to the adsorption of chloride ions or BDC molecules onto the anode surface. It is showed that cathodic and anodic current reduced with the presence of all BDC concentrations and the trend illustrated that these current increased with the rise of BDC concentration. This is evident that additions of BDC concentration subsequently slow down the dissolution process of carbon steel as well as hydrogen evaluation reaction on carbon steel surface. On top of that, the shifted of all E_c

values, either in anodic or in cathodic regions had been determined below 85 mV, which is classifying BDC as a mix type inhibitor.

Based on data in Table 1, the corrosion rate, C_r (mm/yr) has been measured by Equation 1:

$$C_r = I_c.K.W_E/(A.\rho) \quad (1)$$

where I_c (A/cm^2) is the corrosion current density, K is a constant (3272 mm/(A.cm.yr)), W_E (g) is the equivalent weight of carbon steel used, A (cm^2) is the exposed area and ρ (g/cm^3) is the steel density. Both surface coverage, θ and inhibition efficiency, $IE\%$ of BDC were measured by applying Equations 2 and 3:

$$\theta = 1 - I_c'/I_c \quad (2)$$

$$IE\% = 100(1-I_c'/I_c) \quad (3)$$

where I_c' and I_c are the corrosion rate of carbon steel with and without BDC inhibitor, respectively.

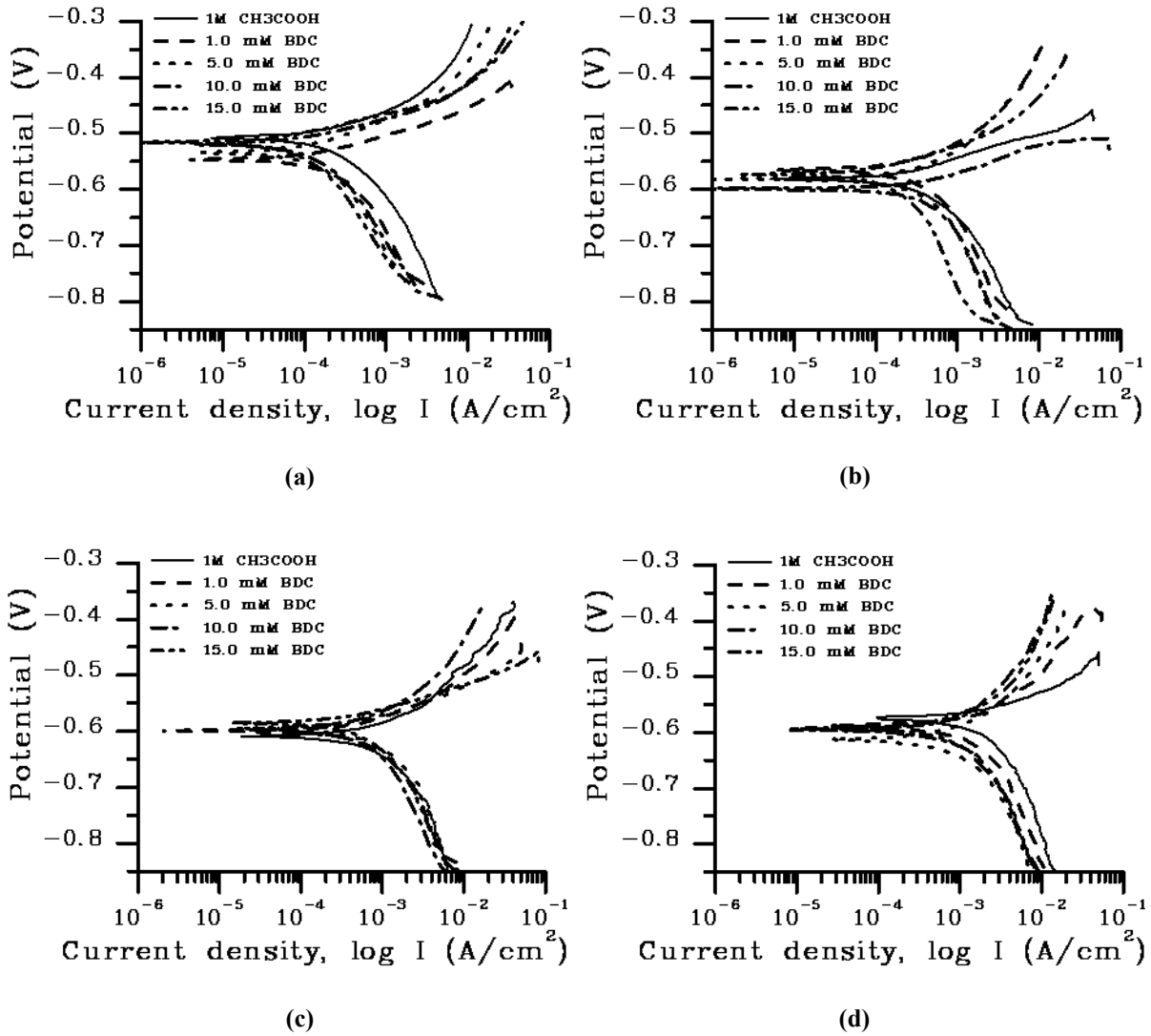
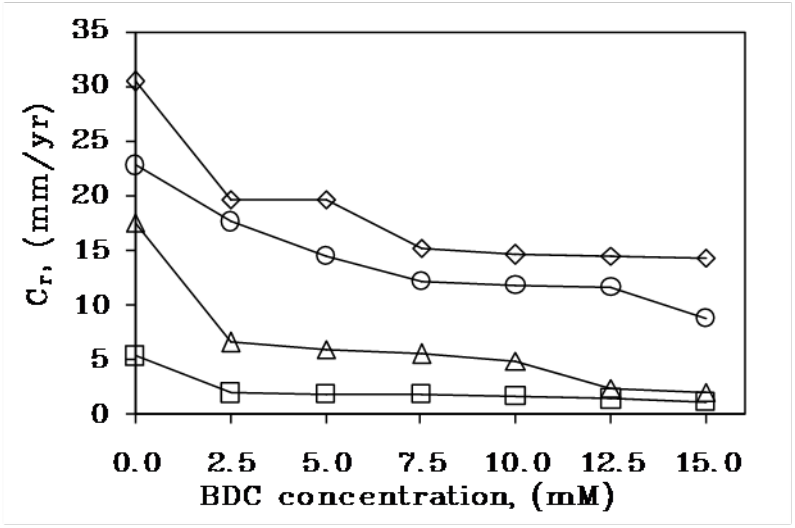


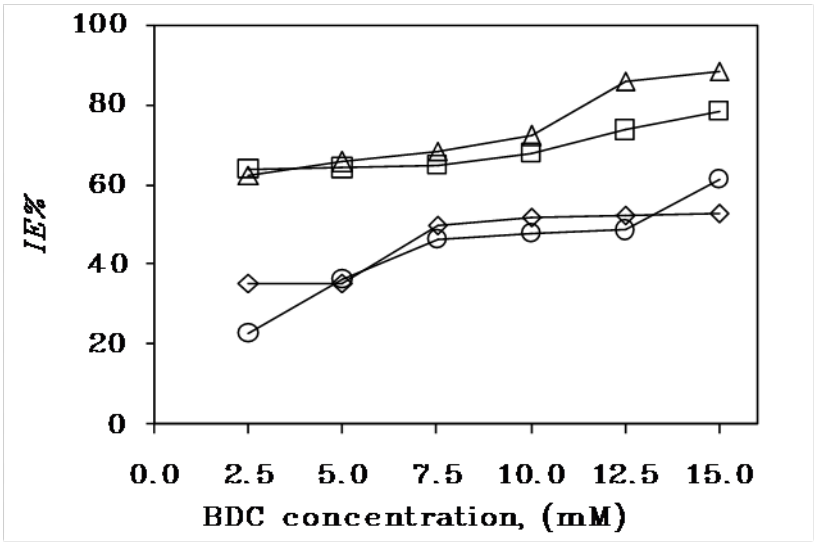
Figure 1: Potentiodynamic polarization curves of different BDC concentration at (a) 25, (b) 40, (c) 55 and (d) 70 °C.

Table 1: Potentiodynamic polarization data for carbon steel corrosion in 1M acetic acid containing different BDC concentration at different temperature.

Temperature (°C)	BDC conc. (mM)	E_c (V)	I_c (mA.cm^2)	$(-)\beta_c$ (V/dec)	β_a (V/dec)
25	0.0	-0.473	0.447	0.322	0.055
	2.5	-0.509	0.162	0.225	0.039
	5.0	-0.523	0.160	0.234	0.064
	7.5	-0.513	0.157	0.229	0.047
	10.0	-0.511	0.144	0.215	0.045
	12.5	-0.507	0.118	0.212	0.041
	15.0	-0.502	0.096	0.215	0.038
40	0.0	-0.570	1.452	0.228	0.050
	2.5	-0.588	0.546	0.340	0.166
	5.0	-0.553	0.500	0.310	0.045
	7.5	-0.584	0.457	0.290	0.045
	10.0	-0.599	0.404	0.300	0.190
	12.5	-0.551	0.202	0.318	0.046
	15.0	-0.515	0.170	0.232	0.055
55	0.0	-0.590	1.891	0.423	0.119
	2.5	-0.573	1.461	0.477	0.045
	5.0	-0.572	1.201	0.379	0.049
	7.5	-0.574	1.011	0.353	0.064
	10.0	-0.621	0.986	0.311	0.192
	12.5	-0.565	0.972	0.345	0.064
	15.0	-0.566	0.728	0.288	0.045
70	0.0	-0.558	2.525	0.380	0.055
	2.5	-0.580	1.634	0.328	0.094
	5.0	-0.619	1.629	0.340	0.212
	7.5	-0.638	1.263	0.308	0.224
	10.0	-0.571	1.212	0.325	0.143
	12.5	-0.626	1.202	0.319	0.219
	15.0	-0.562	1.191	0.330	0.079



(a)



(b)

Figure 2: Analysis of corrosion rate and inhibition efficiency at different BDC concentration in 1 M acetic acid solution at (□) 25, (Δ) 40, (o) 55 and (◊) 70 °C.

Figures 2(a) and 2(b) show the analysis of corrosion rate and inhibition efficiency for all concentrations studied, respectively. As can be seen in Figure 2(a), the corrosion rate values decreased continuously with the addition of BDC concentration. As a result, the inhibition efficiency has also increased with the rise of concentration. Increasing in inhibition efficiency values as a function of concentration suggested that large surface coverage has been produced on steel surface. The maximum IE% values obtained in this study reached up to 90% at optimum temperature 40 °C. This indicates that BDC has a potential to inhibit the corrosion process on the carbon steel surface. At higher concentration, BDC had more tendencies to adsorb and create a thin film to protect the carbon steel from involving active dissolution process.

At 25 °C, the corrosion rate reduced in almost constant at 1.68 mm/yr for all BDC concentration used, as comparison with 1 M acetic acid solution. However, when higher temperatures applied, these values increased gradually for each of BDC concentrations. On top of that, IE% is seen to increase for all BDC concentration from room temperature to 40 °C and definitely diminished at higher temperatures. Obtained experimental results indicated that, BDC molecules had efficiently adsorbed on the steel

surface at temperature 40 °C by substituting water molecules and create a barrier for dissolution of metallic compounds and charge transfer. However, at higher temperatures, the adsorbed BDC molecules obtained enough energy to desorb into bulk solution due to less electrostatic interaction among the ionic charges. This condition reduced the surface coverage and allowed the corrosive medium to take place.

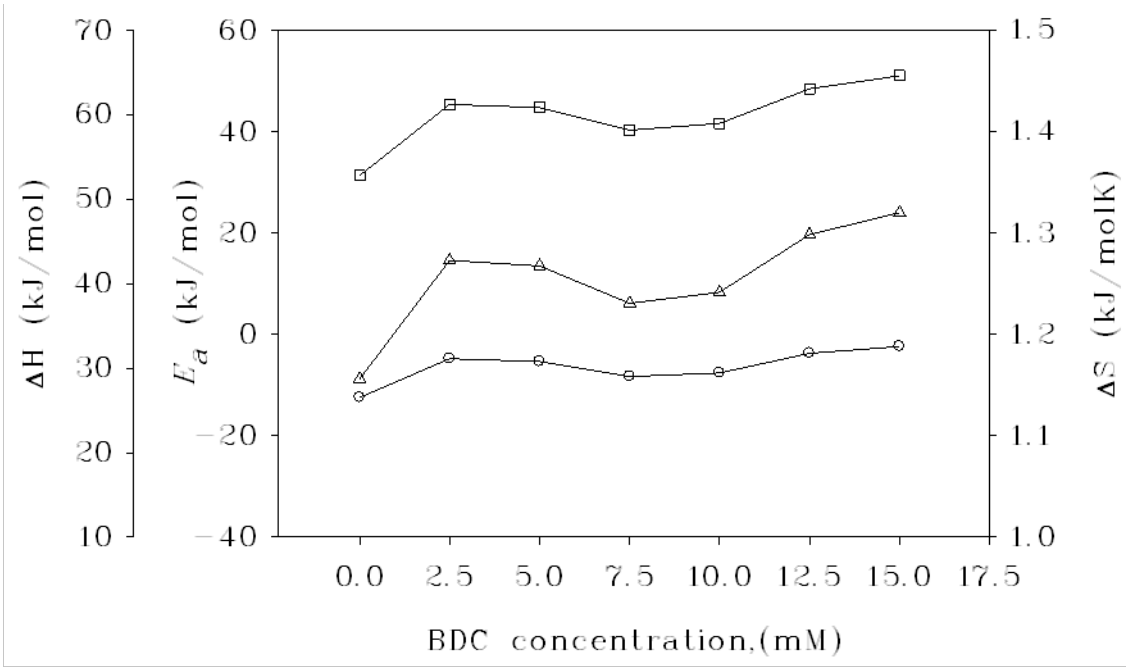


Figure 3: The plots of (□) activation energy E_a, (Δ) activation enthalpy ΔH, and (○) activation entropy ΔS, against BDC concentrations for dissolution process in 1 M acetic acid solution.

The effect of temperature on BDC inhibition efficiency can be quantitatively measured by thermodynamic function. By doing so, type of adsorption can be identified. In this case, Arrhenius equation has been applied to determine the activation energy, E_a (J/mol) of carbon steel dissolution process. This value can be measured by following expression (Behpour *et al.*, 2010):

$$ln\ C_r = ln\ A - E_a/RT \quad (4)$$

where C_r is the corrosion rate, A is the Arrhenius frequency factor, R (8.314 J/mol.K) is the gas constant and T is the absolute temperature. E_a is easily determined from the slope of linear regression between ln C_r and $1/T$. Figure 3 shows the Arrhenius values obtained from different BDC concentration used.

As can be observed in Figure 3, all E_a values with presence BDC inhibitor are higher than uninhibited BDC in1 M acetic acid solution. This result confirmed that the adsorption of BDC molecules onto carbon steel surface is a physisorption process. Increasing of E_a values in the presence of BDC inhibitor can be correlated with the increasing of energy barrier for the corrosion process (Noor & Al-Moubaraki, 2008). The adsorption process is believed to occur due to existing electrostatic force among different cationic charge, N^+ in BDC molecules and the negative charge presence on the steel surface. Anionic charges from acetic acid compound and chloride ions are primary being adsorbed on the steel surface prior to cationic ammonium compound. These associated anionic compounds will become an active platform for BDC to be adsorbed. The interaction of these charges had also been strengthened by pi electrons presence in benzyl group of BDC compound. This adsorption mechanism had potentially made BDC molecules available to form a thin film barrier for inhibiting further dissolution process and definitely increased the E_a values.

In addition to this valuable result, others thermodynamic state functions, which come in consideration are activation enthalpy, ΔH and activation entropy, ΔS. Both state functions can be calculated by the transition state equation (Noor & Al-Moubaraki, 2008):

$$C_r = (RT/Nh)exp(\Delta S/R)exp(-\Delta H/RT) \quad (5)$$

where C_r is the corrosion rate, R is the gas constant, T is absolute temperature, N is the Avogadro number and h is the Plank's constant. Linear plot between $ln\ (C_r/T)$ and $1/T$ will provide a slope and intercept, which the both values of ΔH and ΔS can be measured. These transition state values are shown in Figure 3. The results show that all ΔH are positive in values, suggesting that ions dissolution is an endothermic process. The values of ΔS obtained are relatively low and positive for all BDC concentration used. It can be noticed that, the adsorption of BDC molecules at active surface retarded the corrosion process and minimized the movement of dissolution ions. Both results obtained are in accordance with the E_a values for all concentrations studied. It is showed that BDC is capable of protecting carbon steel surface from actively react with acetic acid medium.

In order to identify the adsorption mechanism of this inhibitor, series of adsorption isotherm models have been carried out and fitted based on the highest correlation coefficient, R^2 value. The result indicated that adsorption process of BDC molecules followed Langmuir adsorption isotherm and the R^2 values for all plots at temperature 25, 40, 55 and 70 $^{\circ}$C were 0.98, 0.96, 0.94 and 0.98, respectively. Langmuir adsorption isotherm was identified by Equation 6:

$$C/\theta = 1/K_{ads} + C \quad (6)$$

where θ is the surface coverage, C is the BDC concentration and K_{ads} is the equilibrium constant of Langmuir adsorption process. It is well known that K_{ads} is related to free adsorption energy, ΔG^o_{ads} by Equation 7 (Benbouya *et al.*, 2012):

$$\Delta G^o_{ads} = -RTln(55.5\ K_{ads}) \quad (7)$$

where 55.5 is the water concentration in solution, R is the molar gas constant and T is the absolute temperature.

Figure 4 shows the graph of Langmuir adsorption isotherm at different temperature. K_{ads} was determined from the intercept of linear regression plot and the value obtained is 0.906, 0.765, 0.211 and 0.379 mM^{-1} for temperature studied at 25, 40, 55 and 70 $^{\circ}$C, respectively. Thus, ΔG^o_{ads} values of these adsorption processes are -26.82, -27.33, -25.55 and -28.38 kJ/mol, respectively. These results revealed that ΔG^o_{ads} values are negative at all temperatures studied, which indicating spontaneous adsorption process. It is well recognized that, ΔG^o_{ads} value lower than -20 kJ/mol is considering as a physisorption process i.e. electrostatic interaction occurs between the adsorbate and adsorbent interface. If the value is more than -40 kJ/mol, it is indicating a charge sharing take place between the inhibitor and active surface of metallic compound namely, chemisorptions (Seifzadeh *et al.*, 2013). The result of ΔG^o_{ads} studied showed that physisoption process dominantly occurred on the carbon steel surface with minor contribution of chemisorptions process as these values obtained in range of -20 and -40 kJ/mol. It is reasonable to suggest that the adsorption mechanism occurred by quasi-substitution between BDC molecules in solution and adsorbed water molecules at the steel surface (Sahin *et al.*, 2002; Tao *et al.*, 2009; Idris *et al.*, 2013). This adsorption process is in good agreement with obtaining result in thermodynamic analysis.

The performance of BDC was also supported by scanning electron microscopic analysis. The morphology of carbon steel immersed in 1 M acetic acid for 6 hours without and with 10 mM BDC is showed in Figure 5. Figure 5(a) presents the micrograph of carbon steel with uninhibited BDC. Strong damage with high corrosion product is seen in most of the carbon steel surface on account of active dissolution process. Whereas, better improvement with less damage on the steel surface can be observed from the micrograph in Figure 5(b), suggesting that good protection has been achieved. It

was confirmed that BDC molecules are able to adsorb on the steel surface and provide passive thin film layer for charges-transferring process. It had also been observed that higher BDC concentration used contribute better surface coverage for protecting corrosion menace. The analysis proved that BDC was capable of inhibiting carbon steel in acetic acid medium.

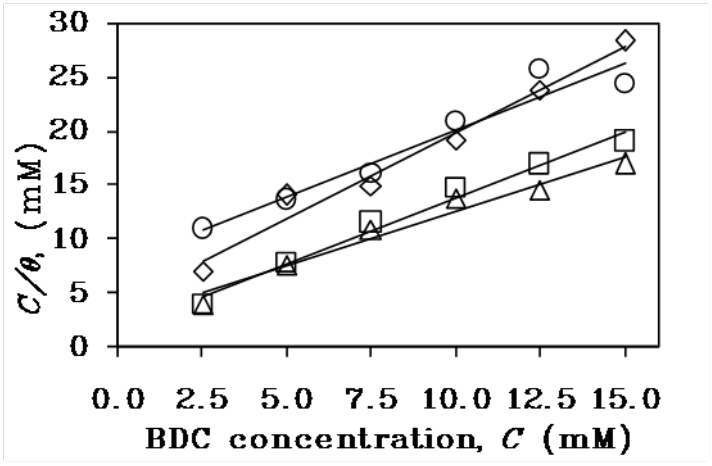
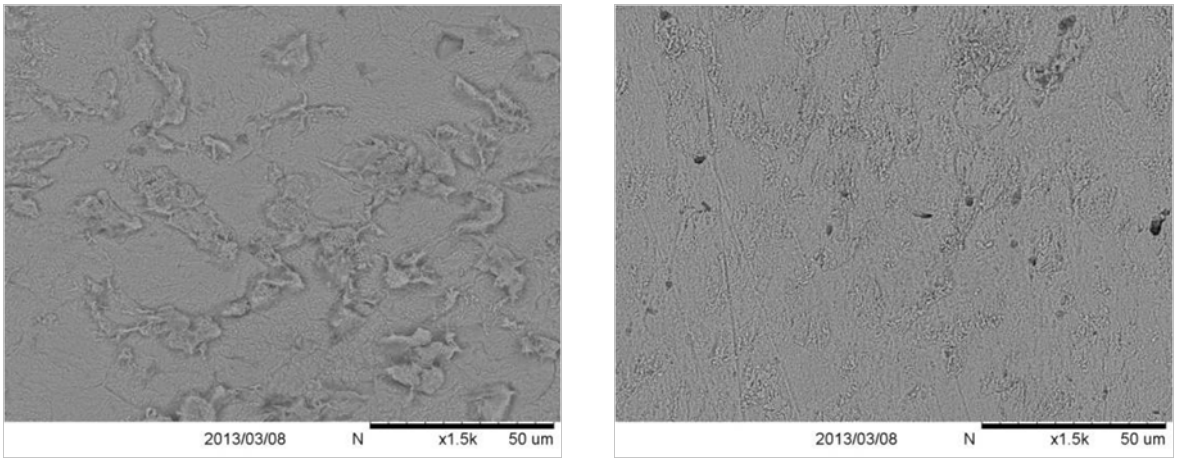


Figure 4: Langmuir adsorption isotherm of BDC on carbon steel at at (□) 25, (Δ) 40, (○) 55 and (◊) 70 ˚C.



(a) **(b)**

Figure 5: Morphology analysis of carbon steel in (a) absence and (b) presence of 10 mM BDC.

4. CONCLUSION

The present study concludes that BDC is able to inhibit the corrosion process of the API5L carbon steel. The inhibition efficiency of this inhibitor had reached up to 90%. Electrochemical analysis indicated that, BDC is a mix type inhibitor and able to inhibit both anodic and cathode side of the carbon steel. It is also proven that inhibition of BDC molecules formed throughout adsorption process, which is in a good agreement with Langmuir adsorption isotherm.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the Ministry of Education Malaysia and Universiti Kebangsaan Malaysia (UKM) for financial support via research grants, ERGS/1/2012/STGS05/ UKM/02/2 and DPP-2013-035. One of the authors would like to acknowledge the Universiti Sains Malaysia (USM) for his study leave.

REFERENCES

Behpour, M., Ghoreishi, S. M., Mohammadi, N., Soltani, N. & Salavati-Niasari, M. (2010). Investigation of some Schiff base compounds containing disulfide bond as HCl corrosion inhibitors for mild steel. *Corros. Sci.*, **52**: 4046-4057.

Belfilali, I., Chetouani, A., Hammouti, B., Aouniti, A., Louhibi, S. & Al-Deyab, S. (2012). Synthesis and Application of 1, 7-bis (2-Hydroxy Benzamido)-4-Azaheptane an Corrosion Inhibitor of Mild Steel in Molar Hydrochloric Acid Medium. *Int. J. Electrochem. Sci.*, **7**: 3997-4013.

Benbouya, K., Zerga, B., Sfaira, M., Taleb, M., Touhami, M. E., Hammouti, B., Benzeid, H. & Essassi, E. (2012). WL, IE and EIS Studies on the Corrosion Behaviour of Mild Steel by 7-substituted 3-methylquinoxalin-2 (1H)-ones and thiones in Hydrochloric Acid Medium. *Int. J. Electrochem. Sci.*, **7**: 6313-6330.

Gece, G. (2011). Drugs: A review of promising novel corrosion inhibitors. *Corros. Sci.*, **53**: 3873-3898.

Idris, M. N., Daud, A. R., Othman, N. K. & Jalar, A. (2013). Corrosion control by benzyl triethylammonium chloride: Effects of temperture and its concentration. *Int. J. Eng. Technol.*, **13**: 47-51.

Mert, B. D., Erman Mert, M., Kardas, G. & Yazici, B. (2011). Experimental and theoretical investigation of 3-amino-1,2,4-triazole-5-thiol as a corrosion inhibitor for carbon steel in HCl medium. *Corros. Sci.*, **53**: 4265-4272.

Mohamad, N., Jalar, A. & Othman, N. K. (2014). Surface morphology study on aluminum alloy after treated with silicate-based corrosion inhibitor from paddy residue. *Sains Malays.*, **43**: 935-940.

Noor, E. A. & Al-Moubaraki, A. H. (2008). Thermodynamic study of metal corrosion and inhibitor adsorption processes in mild steel/1-methyl-4[4'(-X)-styryl pyridinium iodides/hydrochloric acid systems. *Mater. Chem. Phys.*, **110**: 145-154.

Obot, I. B. & Obi-Egbedi, N. O. (2011). Anti-corrosive properties of xanthone on mild steel corrosion in sulphuric acid: Experimental and theoretical investigations. *Curr. Appl. Phys.*, **11**: 382-392.

Popoola, L., Grema, A., Latinwo, G., Gutti, B. & Balogun, A. (2013). Corrosion problems during oil and gas production and its mitigation. *Int. J. Ind. Chem.*, **4**: 35.

Popova, A., Christov, M. & Vasilev, A. (2011). Mono- and dicationic benzothiazolic quaternary ammonium bromides as mild steel corrosion inhibitors. Part II: Electrochemical impedance and polarisation resistance results. *Corros. Sci.*, **53**: 1770-1777.

Raja, P. B. & Sethuraman, M. G. (2008). Natural products as corrosion inhibitor for metals in corrosive media - A review. *Mater. Lett.*, **62**: 113-116.

Sahin, M., Bilgic, S. & Yilmaz, H. (2002). The inhibition effects of some cyclic nitrogen compounds on the corrosion of the steel in NaCl mediums. *Appl. Surf. Sci.*, **195**: 1-7.

Seifzadeh, D., Basharnavaz, H. & Bezaatpour, A. (2013). A Schiff base compound as effective corrosion inhibitor for magnesium in acidic media. *Mater. Chem. Phys.*, **138**: 794-802.

Singh, A., Ebenso, E. E. & Quraishi, M. A. (2012). Theoretical and electrochemical studies of metformin as corrosion inhibitor for mild steel in hydrochloric acid solution. *Int. J. Electrochem. Sci.*, **7**: 4766-4779.

Tao, Z., Zhang, S., Li, W. & Hou, B. (2009). Corrosion inhibition of mild steel in acidic solution by some oxo-triazole derivatives. *Corros. Sci.*, **51**: 2588-2595.

Yahya, S., Othman, N., Daud, A. & Jalar, A. (2013). Surface Morphology Studies of Low Carbon Steel Treated in Aqueous Lignin. *Sains Malays.*, **42**: 1793-1798.

Zhang, Q., Gao, Z., Xu, F. & Zou, X. (2011). Adsorption and corrosion inhibitive properties of gemini surfactants in the series of hexanediyl-1,6-bis-(diethyl alkyl ammonium bromide) on aluminium in hydrochloric acid solution. *Colloid Surf. A*, **380**: 191-200.

MARITIME SECURITY: APPLICATIONS AND PERSPECTIVES TO COMBAT CHEMICAL, RADIOLOGICAL AND EXPLOSIVE THREATS

Fabrizio Pirelli[1,2*], Orlando Cenciarelli[2,3], Valentina Gabbarini[2], Andrea Malizia[2,3], Giuseppe Famà[1], Alessandro Sassolini[2], Fabrizio D'Amico[2,3], Daniele Di Giovanni[2,3], Mariachiara Carestia[2,3], Leonardo Palombi[2,4], Carlo Bellecci[2,3] & Pasquale Gaudio[2,3]

[1]Italian Coast Guard Headquarters, Italy
[2]International Master Courses in Protection against CBRNe events, Department of Industrial Engineering - School of Medicine and Surgery, University of Rome Tor Vergata, Italy
[3]Department of Industrial Engineering, University of Rome Tor Vergata, Italy
[4]Department of Biomedicine and Prevention, School of Medicine and Surgery, University of Rome Tor Vergata, Italy

[*]Email: fabrizio.pirelli@mit.gov.it

ABSTRACT

In a globalised world, the potential for crisis in the exchange of goods through sea routes continues to increase due to its low costs and technological progress. The worldwide terrorist threat has increasingly identified transports as a main target, showing several gaps in the field of security to which international conventions and organisations have tried to find solutions. The development of regulations that has followed the awareness of risks in the maritime sector has determined the creation of a complex organisation attending to prevention procedures and emergency measures. The control of maritime security is based on risk analysis and deterrence measures. This modus operandi, which involves public and private actors with different skills, has allowed the achievement of important results. In this work, we analyse maritime security by discussing the method used for risk assessment of passenger and cargo ships in relation to chemical, radiological and explosive threats, and available technologies that can be used to avoid illicit acts on board ships.

Keywords: *Maritime security; chemical, radiological and explosive threats; risk assessment; mitigation actions; substance riskiness.*

1. INTRODUCTION

Maritime trade has always held a strategic importance for both the economic development of a state and necessary inner supplies. However, transport and navigation activities are characterised by risks and dangers deriving from the nature of shiploads as well as surroundings (King, 2005; Frittelli, 2008; McNicholas, 2008; Kristiansen, 2013). The problems of protection of human lives at sea, ship safety and security of navigation have been addressed with the issuing of international regulations (Mukherjee & Brownrigg, 2013) aimed at the application of modern technologies for construction, navigation and ship equipment, in order to make maritime navigation safer from risks for ships, passengers on board and transported cargos (Motte, 1996; Roach, 2004).

The need to safeguard human lives and shiploads from emerging risks, in particular illicit acts such as terrorist attacks and piracy, has become more and more urgent

(Murphy, 2013; Talley, 2013). In the aftermath of the September 11, 2001 terrorist attack, the need to respond concretely to the growing global terrorist threat has led to, including in the maritime sector, the definition of a new concept of security, understood as physical protection from deliberate illicit acts against the ship itself, passengers and goods on board, and port facilities (Metaparti, 2010). Hence, in this field, security has supported safety in order to safeguard from risks deriving from transport and navigation activities in naturally dangerous surroundings.

The tendency of modern terrorism seems to be "*the lowest number of attacks, the largest number of victims*" (Laruffa, 2009). For this reason, a passenger ship with large number of people on board could represent a terrorist target for both numerous victims and the public impact on the responsible organisation, compromising the security of trades with a spin-off for the economy. Moreover, ships that transport dangerous cargos (e.g., liquefied petroleum gas) could be terrorist targets in a direct way or to cause explosions in port facilities or near the coast with inevitable consequences on population and infrastructures.

In order to combat international illicit acts in the maritime sector, many legislative solutions have been issued to create common standards of protection and defence for both ships and port facilities (Mukherjee & Brownrigg, 2013). In particular, the international standards for maritime security have been first prescribed in 2002as a new chapter (Special Measures to Enhance Maritime Security, Chapter XI-2, SOLAS '74) (IMO, 2002a) in the International Convention for Safety of Life at Sea (SOLAS) (IMO, 1974), which was consolidated as a safety treaty. This addition, together with a detailed code of security, the International Ship and Port Security Code (ISPS Code) (IMO, 2002b), identifies a large juridical structure to defend ships and ports from terrorist attacks through a series of preventive measures (Laruffa, 2009). The norms adopted by SOLAS are of two different types: Chapter XI-2 and Part A of the ISPS Code are the norms of coercive nature, while Part B of ISPS code is constituted by a series of recommendations and orientations that are useful for obligatory application norms that are not mandatory, except the points considered obligatory by Regulation (EC) No 725/2004.Additional regulations for maritime security (e.g., CE 725/2004 (EU, 2004) and CE 65/2005 (EU, 2005)) have further improved prevention procedures and response measures.

In this work, maritime security is analysed, focusing on chemical, radiological and explosive threats. The method used for risk assessment of passenger and cargo ships in relation to these threats, and available technologies that can be used to avoid illicit acts on board ships, are further discussed.

2. RISK ASSESSMENT

As described in the SOLAS and ISPS codes, ships and ports protection is based on the adoption of active and passive measures constructed on three security levels whose application is related to risk assessment (IMO, 2002a, b), and security manoeuvres and devices (e.g., for the ship, the security alert system that communicates the ship's position during piracy attack).The awareness of risk is, undoubtedly, the first step of each assessment. It is important to identify possible threats, their origins and the possible consequences. Essentially, it is necessary to investigate how the item to be protected may be attacked and the occurrence rate. Due to the large number of people on board, a high value of risk for passenger ships has to be assigned; they may be subject to different threats, such as suicide attacks by individuals or groups with explosives, chemical, biological and radiological weapons, and hijacking/hostage-taking, which could lead to the loss of a large number of lives. Nuclear attacks may be practically excluded; although the size of nuclear weapons has decreased considerably

such as that they have become transportable (the so-called 'tactical nuclear weapons'), their distribution and availability is extremely limited.

The second step is the attribution of a level of probability, according to the weaknesses of the ship and the interest to attack it, which could depend on what it transports. Values to be attributed range from 1 to 3, depending on whether the probability of that threat occurring is low (1), medium (2) or high (3).

The third step of the risk assessment is the determination of the ship's vulnerability to the attacks, by assessing the security measures and their effectiveness, the technologies used, and the security personnel's training. Specifically, two factors determine the level of vulnerability: a) accessibility to protected structures in attack scenarios, or any physical barriers that deter threat, and b) the security organisation providing security plans, communication skills, surveillance personnel, intrusion detection systems and timeliness in preventing illicit acts. In this case, the range of values is from 1 to 3, depending on whether the vulnerability is low (1), medium (2) or high (3).Thus, in order to reduce risk, it is necessary to decrease the vulnerability, by identifying all the people who come on board, and installing appropriate barriers that allow accessibility to areas that are fundamental for control and navigation of the ship (e.g. main bridge, engine room, steering gear, emergency batteries room, emergency generator room, etc.) to authorised personnel only.

Finally, it is necessary to assess the impact that could result from an attack. The impact is considered limited (1) when the occurrence of the event would result in minimal effects, both from technical and economic points of view, with short recovery time and no considerable spin-off for politics. The impact level is medium (2) when the consequences, although important, are still moderate in comparison with the maximum level of danger. Finally, the impact level is severe (3) when the consequences are particularly important, with considerable social and political implications, both for the loss of human lives and possible interruption of operating conditions, and the restoration costs.

Considering these premises, it is possible to calculate the risk as the product of the values attributed to the threat, vulnerability and impact:

$$R = T * V * I \qquad (1)$$

where R represents the risk, T represents the threat score, V represents the vulnerability score and I represents the impact score. A minimal score (1) will be assigned in the event of a threat that has a low probability of occurrence, a low vulnerability to be attacked, and limited consequences; whereas a maximum score (27) will be given a threat that has high occurrence probability, high vulnerability and serious impact.

After the risk assessment, it is necessary to define which measures are to be taken in order to mitigate the scenario. For the mitigation actions, a score ranging from 0 (minimum) to 14 (maximum) is assigned. In case of a low event probability, it will be enough to adopt ordinary security measures (score of 0-4) to avoid unnecessary alarms or repercussions on the operations on board. When such measures achieve maximum efficiency, the score attributed is 4. Nevertheless, these measures are improvable (score of 5-9), working on the quality of the equipment used, personnel employed and procedures carried out. Finally, to reduce the risk, additional security measures may be adopted, as well as existing ones (score of 10-14).

By including the mitigation actions score into Equation 1, the real risk for a ship is defined as:

$$ER = R - M \quad (2)$$

where *ER* represents the effective risk, *R* represents the risk as expressed in Equation 1 and *M* represents the mitigation actions score. In the case of maximum risk, even with the most effective mitigations actions, the danger can never be considered completely eliminated. All the steps leading to the final risk assessment can be summarised in the matrix shown in Table 1.

Table 1: Real risk assessment matrix for passenger and cargo ships.

Threat scenario	Possibility of threat ratio *	Vulnera-bility **	Severity of consequences ratio ***	Level of risk	Mitigation actions ****	Real risk
Individual suicide attacks using explosives	1	1	1	1	0	1
			2	2	0	2
			3	3	0	3
		2	1	2	1	1
			2	4	2	2
			3	6	3	3
		3	1	3	2	1
Group suicide attacks using explosives			2	6	3	3
			3	9	4	5
	2	1	1	2	5	0
			2	4	5	0
			3	6	5	1
		2	1	4	6	0
Chemical attacks			2	8	7	1
			3	12	8	4
		3	1	6	7	0
			2	12	8	4
			3	18	9	9
Biological attacks	3	1	1	3	10	0
			2	6	10	0
			3	9	10	0
		2	1	6	11	0
			2	12	12	0
Radiological attacks			3	18	13	5
			1	9	12	0
			2	18	13	5
Hijacking/ hostage taking		3	3	27	14	13

**1, low; 2, medium; 3, high*
***1, low; 2, medium; 3, high*
****1, limited; 2, moderate; 3, severe*
*****0-4, ordinary; 5-9, improved; 10-14, implemented*

3. TECHNOLOGIES TO MITIGATE THREATS

In order to increase the security on board ships, the equipment and technologies used for the detection of terrorist threats have to be strengthened and improved. Several techniques are available to identify substances, compounds or explosive mixtures that can be brought on board (Caygill *et al.*, 2012). As the embarkation of passengers and goods on a ship occurs quickly, the technologies employed must provide quick response and low rate of false positives.

A possible strategy for explosives detection is the use of sniffers (explosive trace detectors, ETDs) (Thomas *et al*., 2007) that utilise a technology based on amplifying fluorescent polymers. Such polymers lose fluorescence when in contact with explosives proportionally to the explosive concentration. The high sensitivity of this tool (in the magnitude of picograms) allows for the detection of explosives present in trace amounts on suspected persons, clothings and items. Furthermore, the ability to detect explosives in the form of vapours makes it feasible to use for inspecting sealed containers. False positives can be easily managed by completing the control process through a detailed inspection of the suspect. The detection results are available within seconds through the reading on a bright display. Moreover, the use of ETD does not require particular technical training for the operator, who can use it with just one hand thanks to the reduced weight and minimum bulk. Considering all these advantages, in order to analyse suspected passengers or baggage, an ETD at each access point of the ship is recommended.

In addition, special equipment for the analysis of liquids is necessary for different access points: these technologies should analyse all the liquids contained in bottles or similar, and provide information related to its potential explosive hazard. A possible solution for this task is represented by Raman spectroscopy, which allows the control of plastic, glass or any other material containers permissive to light passage (Moore & Scharff, 2009). After the identification of a potential risk in a liquid using Raman technologies, it is essential to delegate the analysis to a laboratory for the identification of the substance using different technologies, such as liquid or gas chromatography, coupled with mass spectrometry.

Detection of chemical neurotoxic or vesicant agents can be performed using ion mobility spectrometers (Mäkinen *et al*., 2010) installed at some crucial points in the ship to analyse airborne dusts. It is completely non-invasive and connectable to an alarm system that sorts the signal on the dashboard instrumentation without the need for a qualified operator. Such devices are mainly common for military applications, in which the risk of chemical attack is more concrete, whereas they are still relatively unknown for passenger and cargo ships.

Ion mobility spectroscopy technology is used by chemical agent monitors (CAMs), an automatic detector of chemical, nerve and vesicant weapons. This tool is optimised in a small and handy portable version. However, the presence of a radiation source inside it makes it very dangerous in case of impact or damage, such as by fire. Additional problems could arise for the modalities of the instrument's safekeeping. Therefore, its adoption on board of a passenger ship cannot be recommended, except in cases of particular and specific information about the possible use of chemical weapons.

Another technology for the detection of dangerous chemical agents is flame spectrometry (Seto *et al*., 2005), which uses the specific emissions of organic substances containing sulphur and/or phosphorus during a combustion process in an air/hydrogen flame. This equipment does not use radiation sources, and thus, transportation and safekeeping are very simplified.

Finally, to detect radioactive sources, a Geiger-Muller detector can be used (Gallo *et al*., 2013). Due to its high sensitivity, its utility is not so much to discriminate the type of ionising particle or to obtain information on its energy, but rather to count individual pulses of radiation, even with low ionising power. According to the type of emission, there are Geiger-Muller detectors suitable for α, β or γ particles. A Geiger-Muller detector could be placed inside or immediately after a metal detector portal or an apparatus for security screening of baggages in order to verify the presence of radiation sources at the same time of embarkation. A γ-ray source, diffusible for miles and exclusively dimming with lead plates, could represent a very serious threat aboard a passenger ship, and thus, the use of a Geiger-Muller detector is highly recommended.

4. CONCLUSION

In the aftermath of the September 11, 2001 terrorist attack, security measures that were usually taken and appeared suitable to ensure good governance of the seas have been woefully called into question. The need for safety and security of civil society now imposes that public and private entities do their best, with all the resources at their disposal so that the maritime area and the activities that occur in it do not become a place and instrument of terrorist actions. Therefore, a revolution in the scenario of safety and security has occurred. The approach to the concept of security has changed and new strategies, using tools and technologies that are suitable and effective, have been researched.

In the maritime sector, the potential threats that may involve a ship must be continuously assessed and commensurate with the international geopolitical context. In order to continuously improve the counter measures, it is important to estimate the real risk of a naval unit in a certain context. Adequate personnel training and international cooperation programmes are fundamental to effectively prevent and combat terrorist threats. In this manner, operational and technical knowledge in the field of maritime safety can be extended and implemented. Particular attention should be paid to emerging threats, arising from the use of biological, chemical, radiological or explosive (CBRNe) agents. In this context, at the University of Rome Tor Vergata, a team of experts is involved in the training of first responders and decision makers for CBRNe events (Cenciarelli *et al*., 2013a, b, 2014; Pazienza *et al*., 2013, 2014; Di Giovanni *et al*., 2014; Malizia *et al*., 20110, 2011, 2012; Cacciotti *et al*., 2014; Sassolini *et al*., 2014).

A passenger ship represents an attractive target for terrorists, due to the large number of people on board: for this reason, the level of risk is considered high and hence, it is essential to act by increasing security measures, using the latest technology and training staff carefully. To this end, equipment for liquids analysis, radiation sources control, and explosives and chemical weapons detection represent a useful solution to reduce the risk threshold to within the acceptable safety level.

In order to prevent threats in the maritime sector, it is absolutely recommended the installation of specific equipment at each point of access on the ship. Currently, several techniques to quickly identify CBRNe agents, without the need for skilled operators, are available. In particular, ETD allows for explosives detection with high specificity and sensibility. For the analysis of liquids, a possible strategy to be used is Raman spectroscopy, which provides information about the potential riskiness as explosive. Ion mobility and flame spectrometries are useful to detect dangerous chemical agents illicitly brought on board for terrorist purposes. Finally, Geiger-

Muller detectors are suitable to detect radiation sources that are very dangerous for health.

It is important to note that the identification of substance riskiness is not enough; the analysis must continue in a laboratory ashore, using additional technologies for accurate determination of the suspicious substance. The choice of the most suitable equipment to combat all the possible threats that could involve a ship is not easy. Boarding of the ship is the most delicate stage, whereby balancing security with the limited time of embarkation represents the goal to be reached.

REFERENCES

Cacciotti, I., Aspetti, P.C., Cenciarelli, O., Carestia, M., Di Giovanni, D., Malizia, A., D'Amico, F., Sassolini, A., Bellecci, C. & Gaudio, P. (2014). Simulation of Caesium-137 (^{137}Cs) local diffusion as a consequence of the Chernobyl accident using Hotspot. *Defence S&T Tech. Bull.,* **7**:18-26.

Caygill, J.S., Davis F. & Higson, S.P.J. (2012). Current trends in explosive detection techniques. *Talanta,* **88**:14-29.

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. (2014). Biological emergency management: the case of Ebola 2014 and the air transportation involvement. *J. Microb. Biochem. Technol.*, **6**: 247-253.

Cenciarelli, O., Malizia, A., Marinelli, M., Pietropaoli, S., Gallo, R., D'Amico, F., Bellecci, C., Fiorito, R., Gucciardino, A. & 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.

Di Giovanni, D., Luttazzi, E., Marchi, F., Latini, G., Carestia, M., Malizia, A., Gelfusa, M., Fiorito, R., D'Amico, F., Cenciarelli, O., Gucciardino, A., Bellecci, C. & Gaudio, P. (2014).Two realistic scenarios of intentional release of radionuclides (Cs-137, Sr-90) - the use of the HotSpot code to forecast contamination extent. *WSEAS T. Environ. Dev.,* **10**:106-122.

EU (European Union) (2004). Regulation (EC) No. 2004/725/EC of the European Parliament and of the Council on enhancing ship and port facility security. *Official J.Eur. Union*, **L129**:6-91.

EU (European Union) (2005). Regulation (EC) No. 2005/65/EC of the European Parliament and of the Council on enhancing port security. *Official J. Eur. Union*, **L310**:28-39.

Frittelli, J.F. (2008). Maritime security: Overview of issues.*In*Vesky, J.P. (Ed.),*Port and Maritime Security*. Nova Science Publishers Inc., New York.

Gallo, R., De Angelis, P., Malizia, A., Conetta, F., Di Giovanni, D., Antonelli, L., Gallo, N., Fiduccia, A., D'Amico, F., Fiorito, R., Richetta, M., Bellecci, C. & Gaudio, P. (2013). Development of a georeferencing software for radiological diffusion in order to improve the safety and security of first responders. *Defence S&T Tech. Bull.,***6**:21-32.

IMO (International Maritime Organization). (1974). *International Convention for the Safety of Life At Sea.* International Maritime Organization (IMO), London.

IMO (International Maritime Organization). (2002a). *International Convention for the Safety of Life At Sea, IMO activities to enhance maritime security, Conference of Contracting Governments to the International Convention for the Safety of Life at Sea*. International Maritime Organization (IMO), London.

International Maritime Organization (IMO). (2002b). *International Ship & Port Facility Security Code and SOLAS Amendments 2002*. International Maritime Organization (IMO), London.

King, J. (2005). The security of merchant shipping. *Mar. Pol.*, **29**:235-245.

Kristiansen, S. (2013). *Maritime Transportation: Safety Management and Risk analysis.* Routledge, Taylor & Francis Group, London, United Kingdom.

Laruffa, V. (2009). Prospettive della sicurezza in ambito marittimo: infrastrutture critiche e dimensione marittima della security. *Ricerca CeMISS 2009*, Centro Militare di Studi Strategici (CeMISS), Rome, Italy.

Mäkinen, M.A., Anttalainen, O.A. & Sillanpää, M.E. (2010). Ion mobility spectrometry and its applications in detection of chemical warfare agents. *Anal.Chem.*, **82**:9594-9600.

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

Malizia, A., Quaranta, R., Mugavero, R., Carcano, R., & Franceschi, G. (2011). Proposal of the prototype RoSyD-CBRN, a robotic system for remote detection of CBRN agents. *Defence S&T Tech. Bull.*, **4**:64-76.

Malizia, A., Quaranta, R., & Mugavero, R. (2010). CBRN events in the subway system of Rome: Tecnhical-managerial solutions for risk reduction. *Defence S&T Tech. Bull.*, 3:140-157.

McNicholas, M. (2008). *Maritime Security: an Introduction.* Elsevier, Burington, Massachusetts.

Metaparti, P. (2010). Rhetoric, rationality and reality in post-9/11 maritime security. *Maritime Pol. Manag.*, **37**:723-736.

Moore, D.S. & Scharff, R.J. (2009). Portable Raman explosives detection. *Anal. Bioanal. Chem.*, **393**:1571-1578.

Motte, R. (1996). Safe navigation, ship loss and applications of technology. *J. Navigation*, **49**:36-44.

Mukherjee, P. K., & Brownrigg, M. (2013). *Farthing on International Shipping*. Springer, Berlin.

Murphy, M. N. (2013). *Contemporary Piracy and Maritime Terrorism: The Threat to International Security*. Routledge, Taylor & Francis Group, London, United Kingdom.

Pazienza, M., Britti, M.S., Carestia, M., Cenciarelli, O., D'Amico, F., Malizia, A., Bellecci, C., Gaudio, P., Gucciardino, A., Bellino, M., Lancia, C., Tamburrini, A. & Fiorito, R. (2013). Application of real-time PCR to identify residual bio-decontamination of confined environments after hydrogen peroxide vaportreatment: Preliminary results. *J. Microb. Biochem. Technol.*, **6**:24-28.

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.

Roach, J.A. (2004). Initiatives to enhance maritime security at sea. *Mar. Policy*, **28**:41-66.

Sassolini, A., Malizia, A., D'Amico, F., Carestia, M., Di Giovanni, D., Cenciarelli, O., Bellecci, C., Gaudio, P. (2014) Evaluation of the effectiveness of titanium dioxide (TiO_2) self-cleaning coating for increased protection against CBRN incidents in critical infrastructures. *Defence S&T Tech. Bull.,***7**:9-17.

Seto, Y., Kanamori-Kataoka, M., Tsuge, K., Ohsawa, I., Matsushita, K., Sekiguchi, H., Itoi, T., Iura, K., Sano, Y. & Yamashiro, S. (2005). Sensing technology for chemical-warfare agents and its evaluation using authentic agents. *Sensor. Actuat. B: Chem.*, **108**:193-197.

Talley, W. (Ed.). (2013). *Maritime Safety, Security and Piracy*. CRC Press, LCC, Florida, USA.

Thomas, S.W., Joly, G.D. & Swager, T.M. (2007). Chemical sensors based on amplifying fluorescent conjugated polymers. *Chem. Rev.*, **107**:1339-1386.

DEVELOPMENT OF A LABORATORY SCALE REMOTELY OPERATED VEHICLE (ROV) USING LEGO MINDSTORMS

Che Wan Mohd Noor[1*], Mahdi Che Isa[2], Khalid Samo[3] & Amanda Cheng Man Dee[1]

[1]School of Ocean Engineering, Universiti Malaysia Terengganu (UMT), Malaysia
[2]Marine Materials Research Group, Maritime Technology Division (BTM), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[3]Faculty of Applied Sciences, Universiti Teknologi MARA (UiTM), Malaysia

[*]Email: che.wan@umt.edu.my

ABSTRACT

This paper discusses the design and development of a laboratory scale remotely operated vehicle (ROV) using Lego Mindstorms. The prototype ROV is a compact unit built using a limited number of components and is suitable for underwater inspection using a web camera. The ROV's operational efficiency and performance was evaluated based on its ability to move forwards and backwards, ascending and descending rates, and turning radius with respect to motor speed. Reverse engineering was used to identify manoeuvring problems before modifications were made. The size of the propulsion motors and propellers to propel the ROV were calculated and recommended theoretically.

Keywords: *Remotely operated vehicle (ROV); Lego Mindstorms; dry and underwater manoeuvring tests; propeller thrust; drag force.*

1. INTRODUCTION

Advancements in technology in this day and age have led to the creation of robots to increase work efficiency and reduce human workload. A remotely operated vehicle (ROV) is a highly manoeuvrable tethered underwater robot that operates in response to human commands (Christ & Wernli, 2007; Shepherd, 2009). They are made for underwater exploration, recoveries, inspections, search and rescue, trenching, cable burial, and much more. ROVs are connected to the surface platform by a cable or umbilical cord that provides power and control communications. ROVs may sometimes be called remotely operated underwater vehicle to distinguish it from remote control vehicles operating on land or in the air (Azis *et al.*, 2012).

The use of autonomous underwater vehicles (AUVs) and ROVs for subsea measurements and monitoring as well as other tasks are rapidly growing (Robinson & Keary, 2000; Christ & Wernli, 2007). In Malaysia, there is a large demand of ROVs for underwater applications, particularly in the oil and gas industry. Contractors have been depending on foreign makers or suppliers for ROVs. To this end, efforts are emerging to develop ROV prototypes by local companies.

Despite advanced specifications of ROVs, researches are continuing to improve their performances and capabilities beyond standard usage, such as inspection and maintenance in the offshore oil industry, mine hunting, mapping, and marine research. Generally, the motivation for developing a ROV has been the desire to eliminate or reduce the need for divers as this involves safety, endurance and cost. ROVs are designed based on sub-systems and operators need to understand the entire system before they are able to control and manipulate a ROV from a surface vessel. ROVs can vary in size from small vehicles with video for simple observation up to complex systems, which can have several dexterous manipulators, TVs, video

camera, tools and other equipment (von Alt *et al*., 1994; Frost *et al*., 1996; Nakamura *et al*., 2001; Christ & Wernli, 2007; Azis *et al*., 2012).

The aim of this study is to design and develop a laboratory scale ROV using Lego Mindstorms. Lego Mindstorms is a line of programmable robotics that comes in a kit containing many pieces, including sensors and cables (Erwin, 2001; Ferrari *et al*., 2002). The operational efficiency of the constructed prototype ROV is evaluated based on its movements and speed in a test tank with respect to motor speed. The ROV is fitted with a web camera and sensors for underwater inspection.

2. DESIGN OF THE PROTOTYPE ROV

The constructed prototype consisted of the primary components shown in Figure 1. The computer and the NXT Intelligent Brick, which is a programmable Lego brick, are used to control the ROV, which has built-in webcam, motors, sensors, etc.

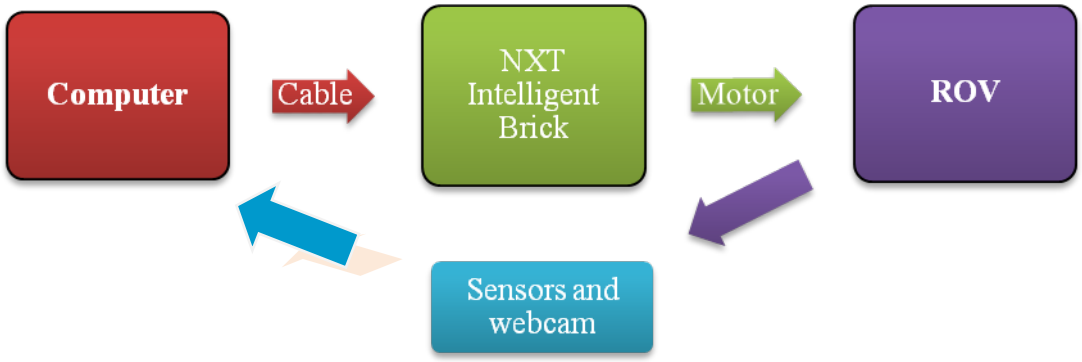


Figure 1: The primary components and control flow of the prototype ROV.

This design involved programming using Lego Mindstorms NXT 2.0, which provides a visual programming language for writing simple instructions and uploading them to the NXT Brick. Lego Mindstorm employs command box programming. Figure 2 shows the program designed for the ROV. The light emitter graphic in the program is used to control the light emitting function of the ROV when it is in operation, while the light sensor graphic is used to detect and record the surrounding brightness of the environment during underwater inspections. This function allows the ROV to sense the presence of obstacles that allows the user to manoeuvre the ROV more cautiously or manoeuvre away from the obstacles. The remote control function is used to control the motors of the ROV remotely. A Cyberlink YouCam web camera, which is easily available in the market, was incorporated into the ROV to capture and record images and video.

A container made of plastic material was used as the housing where all the ROV's electronics, including motors and batteries, are packed together. The NXT Brick was given extra protection by wrapping it using a plastic sheet. Three identical servomotors with reduced gear assemblies were used to propel the ROV. The internal optical rotary encoders sense the motor rotations within one degree of accuracy.

Figure 3 shows the propellers and motors fitted onto the ROV. Two bladed propellers, with diameter of 38 mm and made of plastic, were chosen to propel the ROV because they are cheap and suitable for small brushed electric motors. One motor runs two propellers that are set vertically. Two horizontal thrusters, fitted at the rear of ROV, are used. They are connected and

driven by individual motors. In order to move forwards and backwards, the motors are controlled to move in the required directions (Table 1). With this configuration, the ROV is able to move in three dimensional spaces. Four propeller shafts, with length of 55 mm and diameter of 4 mm, were used to connect the propellers and motors.

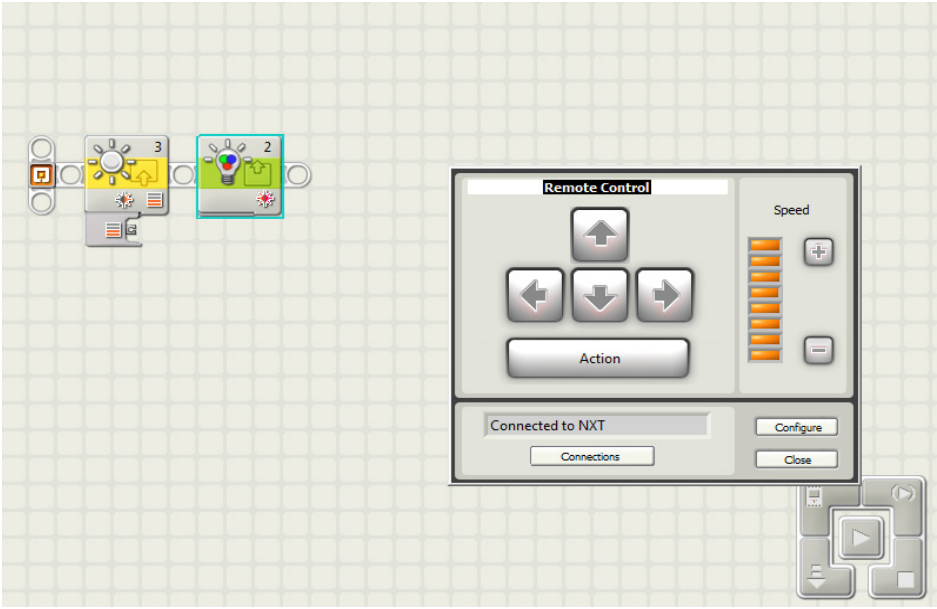


Figure 2: The Lego Mindstorms NXT 2.0 ROV program.

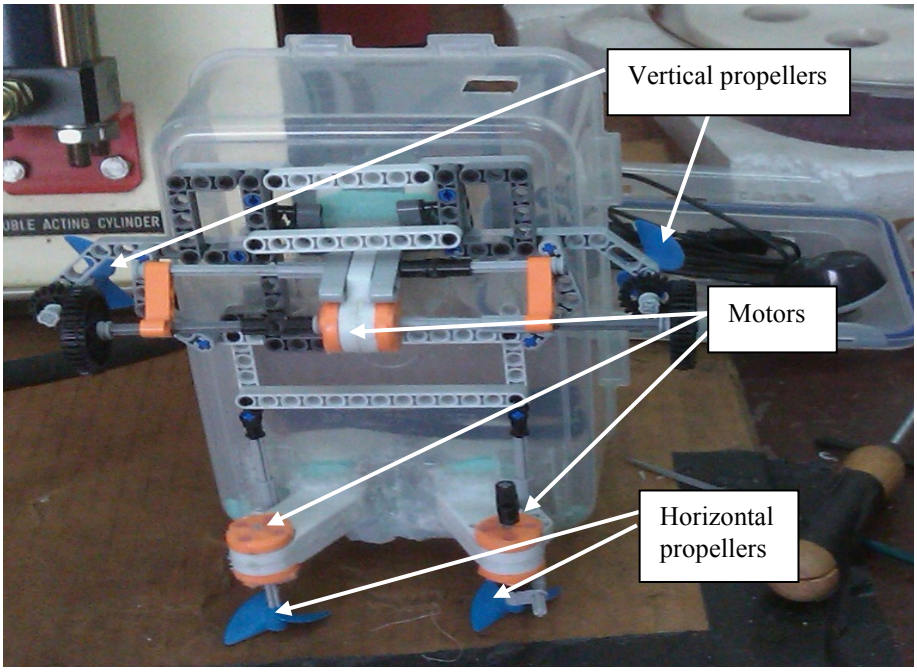


Figure 3: The ROV's propellers and motors configuration.

Table 1: Control of movements of the ROV by varying the speeds and directions of the motors.

ROV movement	Left propeller (horizontal)	Right propeller (horizontal)
Forward	Clockwise	Anticlockwise
Backward	Anticlockwise	Clockwise
Left	Stop	Anticlockwise
Right	Clockwise	Stop
Forward left	Clockwise: Half speed	Anticlockwise
Forward right	Clockwise	Anticlockwise: Half speed
Backward left	Anticlockwise: Half speed	Clockwise
Backward right	Anticlockwise	Clockwise: Half speed
ROV movement	**Left propeller (vertical)**	**Right propeller (vertical)**
Up	Clockwise	Clockwise
Down	Anticlockwise	Anticlockwise

Figure 4 shows the ROV's internal equipment configuration. For the ROV to collect data or react to its environment, a light sensor detects the light level in one direction while a light-emitting diode (LED) illuminates the object. For the LED to illuminate the object and the web camera to view it from the casing, a square hole was made in the housing and a clear glass was fitted to cover the opening. For buoyancy control and to keep the ROV in the right orientation, syntactic foam and weight (lead with varying values from 0.01 to 0.1 kg) were used to fill the case based on hydrostatic calculations. The ROV was designed to have slight positive buoyancy and, in the case of malfunction, will rise to the surface. The lid of the case and any other holes made for the control system, power cords, glass opening and shafts were sealed with silicone sealant. The whole ROV system is powered by six AA alkaline batteries.

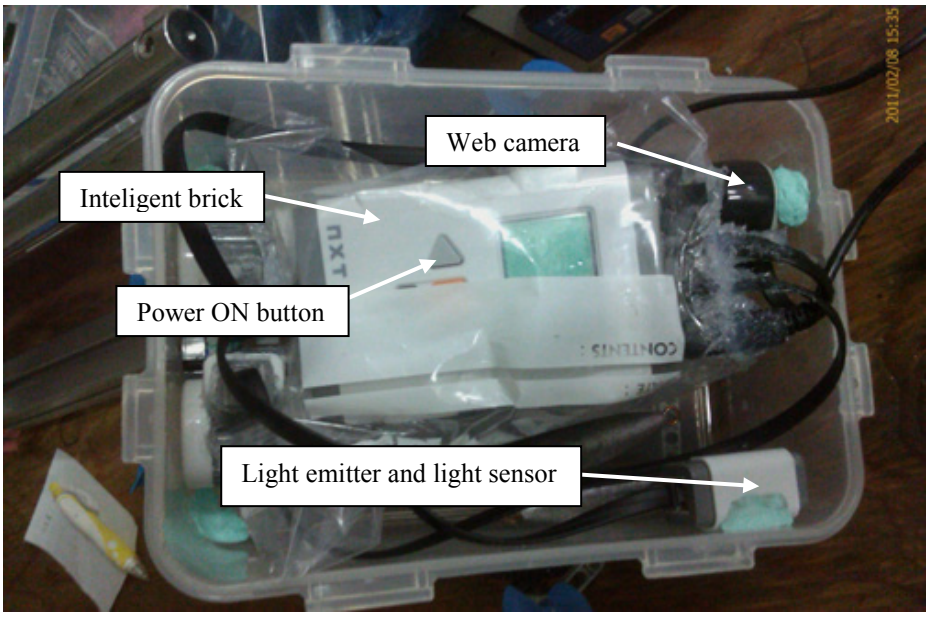


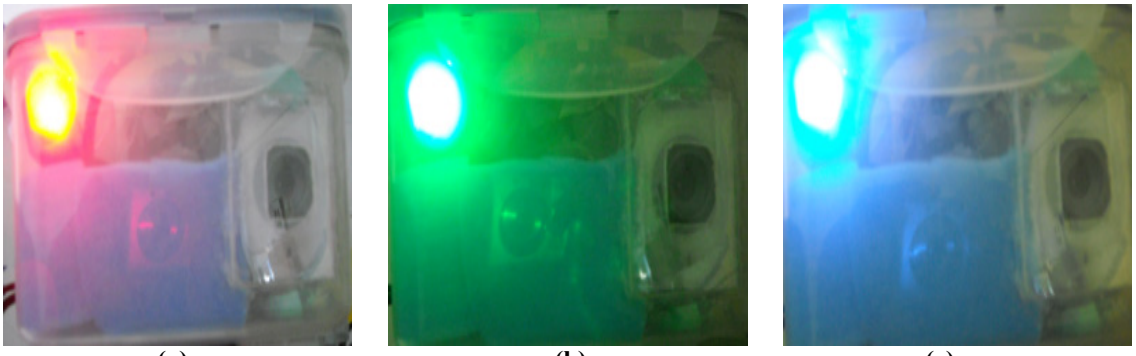
Figure 4: The ROV's internal equipment configuration.

3. EVALUATION OF THE PROTOTYPE ROV'S OPERATIONAL EFFICIENCY

A dry test was carried out to ensure the operation of all controls, including the functionality of all sensors and web camera. Evaluation of the ROV's operational efficiency was then conducted based on its forward and backward movements, ascending and descending rates, and turning radius with respect to motor speed when tested in a test tank.

3.1 Dry Test

The ROV's control system responded well during the dry test. Figure 5 shows the light emitting test for the ROV's light emitter, where it emitted red, green and blue lights as controlled by the user. Figure 6 shows the results of the light sensor test, with the graph showing the percentage of light changes detected by the light sensor over the period of 1 min; 0 % indicates total darkness, while 100 % indicates a bright condition for the ROV to collect data of the surrounding environment. The light percentage decreased in the first 10 s when the ROV moved closer to a tank's wall, and increased in the next 10 s when it moved away from the wall. Between the periods of 40 to 50 s, the light intensity was at the highest when light was beamed towards the light sensor. Figure 7 shows the images captured by the web camera during the ROV's dry and underwater tests.



(a) (b) (c)

Figure 5: The ROV's light emitter emitting (a) red, (b) green and (c) blue lights.

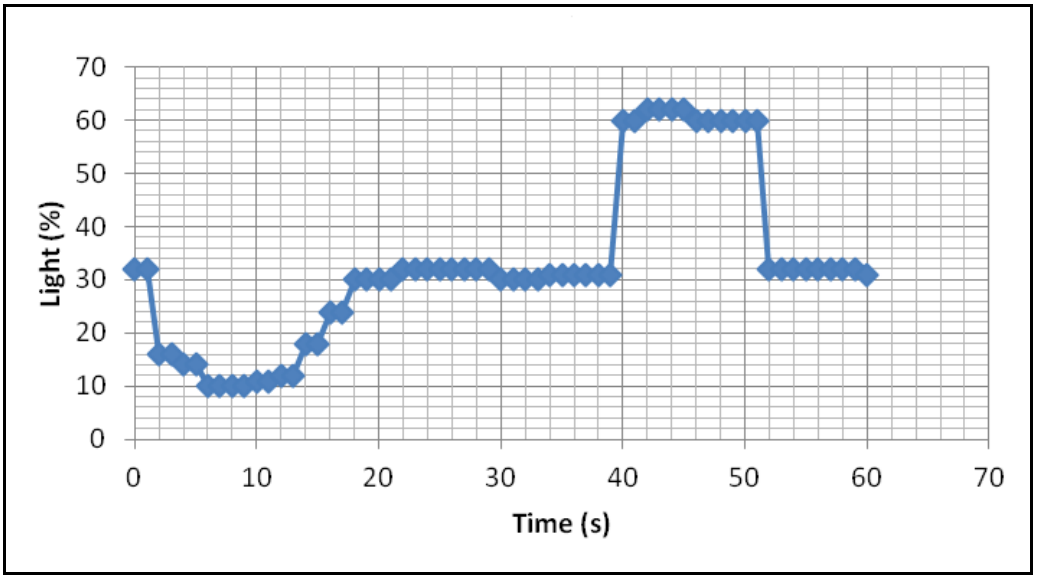


Figure 6: Percentage of light changes detected by the light sensor over the period of 1 min.

(a) (b)

Figure 7: Images captured by the web camera for the (a) dry and (b) underwater tests.

3.2 Underwater Manoeuvring Test

The ROV was designed to have slight positive buoyancy, for which 3.05 kg of well distributed weight was added. When the ROV was tested in the water, there was not enough thrust from the motor and propellers to move the ROV forwards and backwards, turn, and dive as the power could not overcome the drag force in the water. The results of computation of drag force against velocity for different hull shapes are shown in Figure 8, with the prototype ROV being cubic shaped.

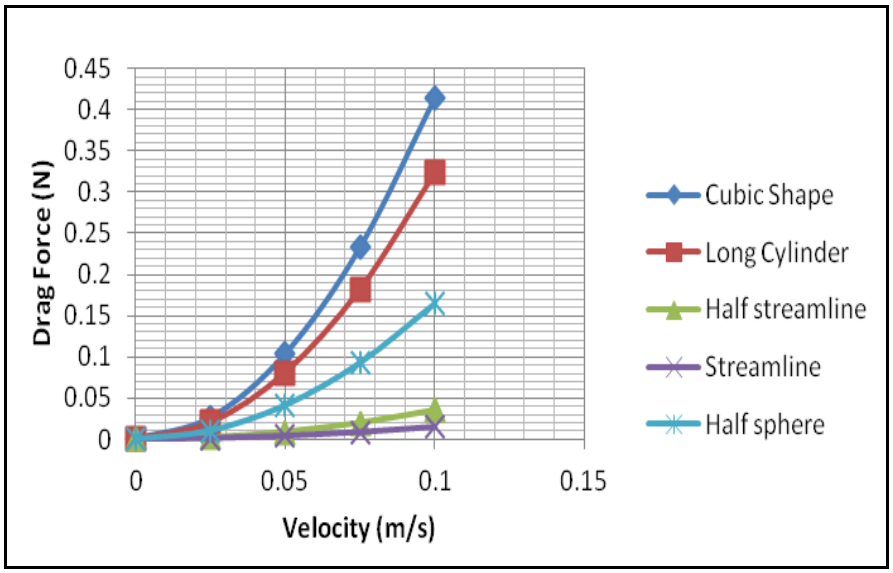


Figure 8: Results of computation of drag force against velocity for different hull shapes.

Figure 9 shows the graph of the propeller thrust calculated compared to the ROV's drag force. It is observed that the thrust provided by the motors and propellers was not able to propel the ROV or overcome the drag force. To solve this problem, it is proposed that a new 3 bladed propeller, with diameter of 50 mm and angle of blade slope of 42°, be added. Based on this change, Figure 10 shows that the propeller thrust calculated can overcome the drag force for the ROV to move forwards and backwards, turn, and dive. In addition, a more streamlined housing, such as using half sphere shape, would certainly reduce the ROV's drag force.

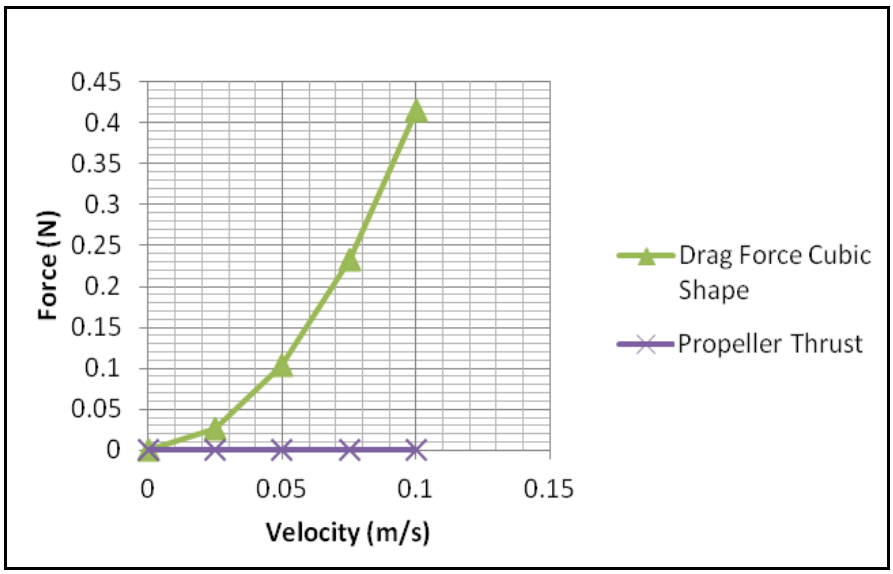


Figure 9: Comparison of the ROV's propeller thrust and drag force.

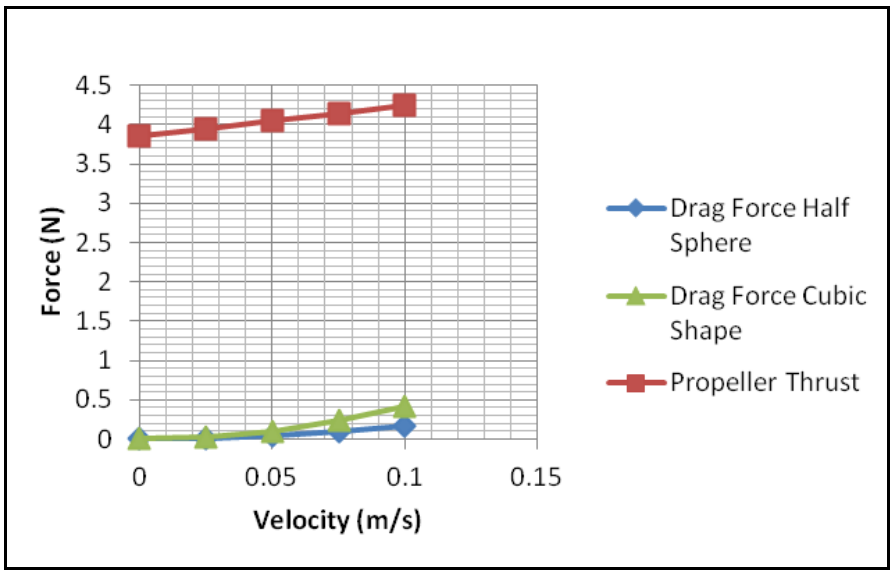


Figure 10: Comparison of the ROV's propeller thrust and drag force after addition of the new propeller.

4. CONCLUSION

The ROV used in this study was powered solely by a programmable LEGO intelligent brick and was primarily assembled using standard LEGO components. This ROV is very compact, containing only a limited number of components. While the ROV functioned successfully in the dry test, the underwater manoeuvring tests were a failure. This was due to the ROV's propeller thrust being insufficient to overcome the drag force. The new proposed propeller was shown able to produce sufficient propeller thrust to overcome the drag force.

REFERENCES

Azis, F.A., Aras, M.S.M., Rashid, M.Z.A., Othman, M.N. & Abdullah, S.S. (2012). Problem identification for underwater remotely operated vehicle (ROV): A case study. *Procedia Eng*., **41**: 554-560.

Christ, R. & Wernli, R. (2007). *The ROV Manual*. Butterworth Heinemann, Oxford.

Erwin, B. (2001). *Creative Projects with LEGO Mindstorms*. Addison-Wesley, Boston, Massachusetts.

Ferrari, M., Ferrari, G. & Hempel, R. (2001). *Building Robots with LEGO Mindstorms: The Ultimate Tool for Mindstorms Maniacs*. Syngress, Boston, Massachusetts.

Frost, A.R., McMaster, A.P., Saunders, K.G. & Lee S.R. (1996). The development of a remotely operated vehicle (ROV) for aquaculture. *Aquacult. Eng.*, **15:** 461-483.

Nakamura, M., Kajiwara, H. & Koterayama, W. (2001). Development of an ROV operated both as towed and self-propulsive vehicle. *Ocean Eng.*, **28**: 1-43.

Christ, R. & Wernli, R. (2007). *The ROV Manual: A User Guide for Observation-Class Remotely Operated Vehicles*. Elsevier Ltd., Oxford.

Robinson, H. & Keary, A. (2000). Remote control of unmanned undersea vehicles. *Int. Unmanned Undersea Vehicle Symp.*, pp. 24-28.

Shepherd, K. (2009). Remotely operated vehicles (ROVs). *In* Steele, J.H., Turekian, K.K. & Thorpe, S.A. (Eds.) *Encyclopaedia of Ocean Sciences*. Waltham, Massachusetts, pp. 742-747.

von Alt, C., Allen, B., Austin, T. & Stokey, R. (1994). Remote environmental measuring units. *Proc. 1994 Symp. Auton. Underwater Vehicle Tech. (AUV '94)*, pp. 13-19.

STUDY OF NOISE EXPOSURE INSIDE A MALAYSIAN ARMY THREE-TONNE TRUCK DRIVER'S COMPARTMENT USING I-KAZ^{TM}

Shamsul Akmar Ab Aziz[1,2,*], Mohd Zaki Nuawi[1], Mohd Jailani Mohd Nor[1] & Dian Darina Indah Daruis[3]

[1]Department of Mechanical and Material Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia (UKM), Malaysia
[2]Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[3]Universiti Pertahanan Nasional Malaysia (UPNM), Malaysia

[*]E-mail: shamsulakm@gmail.com

ABSTRACT

Prolonged and excessive exposure to noise inside truck cabins can cause long term harm and adverse effects to drivers. To this end, the objective of this study was to monitor noise exposure at the driver's ear level while driving a Malaysian Army (MA) three-tonne truck using the Integrated Kurtosis-based Algorithm for Z-notch Filter (I-kaz^{TM}) statistical analysis method. The recorded raw noise exposure data was analysed using I-kaz^{TM} to provide the I-kaz^{TM} coefficient Z^{∞} and I-kaz^{TM} display, which is a 3D graphical representation of the degree of data scattering. It was found that increase of sound pressure level SPL and truck speed result in increase of data scattering in the I-kaz^{TM} display and value of Z^{∞}. This study demonstrates that I-kaz^{TM} is a very effective method for noise monitoring as it can detect SPL changes that are very small.

Keywords: *Noise monitoring; Integrated Kurtosis-Based Algorithm for Z-notch Filter (I-kaz^{TM}); sound pressure level; truck speed; data scattering.*

1. INTRODUCTION

Noise-induced hearing loss is one of the most common occupational disabilities due to extremely loud noises or prolonged exposure to noise. Exposure to loud noise, even for a few minutes, can cause temporary hearing loss. If the exposure is repeated over time, recovery decreases and eventually, the temporary degradations become permanent. Individual susceptibility to noise-induced hearing loss varies widely. Some of these health effects include increased risk of cardiovascular disease, and negative effects on sleep, communication, performance, behaviour, reading, memory acquisition and mental health (DOD, 1993). Furthermore, many studies have demonstrated the impact of decreased communication due to noise exposure on vehicle operations (Nakashima *et al*., 2007; Weatherless *et al.* 2012).

The basic steady state noise criterion for conservation of hearing is that unprotected personnel should not be exposed to noise levels that are higher than 85 dB(A) for a duration of 8 h (DOD, 1991, 1993; DHHS, 1998). Prolonged exposure to noise levels above 85 dB(A) can damage inner ear cells and lead to hearing loss. Research has shown that noise is one of the leading causes of hearing loss for millions of people with impaired hearing in the U.S. In addition, noise can change a man's physiological state by speeding up pulse and respiratory rates. According to medical studies, there is an increased risk to the cardiovascular system from sound pressure levels of above 65 dB (A) (Fooladi, 2012).

Hearing loss is a widespread, severe and costly problem to many military veterans returning from service (Humes *et al*., 2006), with the precise mechanisms and full impact of hearing loss on dismounted operations remaining uncertain (Weatherless *et al*., 2012). The Malaysian Armed Forces (MAF) Medical Board reported that an increasing number of MAF personnel and veterans are suffering from hearing problems, with 22% of them found to be suffering from the problem between

2000 and 2008 (Bernama, 2011). Most importantly, hearing loss degrades the soldier's ability to understand direct commands and radio messages, making it more difficult for the soldier to operate as a member of a squad and increasing the soldier's vulnerability. In addition, reduced hearing ability creates situational awareness problems for soldiers operating on the battlefield (Humes *et al.* 2006). Radio communications further increase the noise exposure at the ear because operators tend to increase the volume to hear the speaker over the background noise (Pääkkönen & Lehtomäki, 2005).

Vehicle interior noise inside the driver's cabin is a combination of engine, road, intake and exhaust, aerodynamics, components and ancillaries, and brakes. Noise and vibration also originates from outside the vehicle, interacting with the vehicle structure and then producing radiated sound inside the driver's cabin. Vehicle noise can cause hearing loss, and discomfort and annoyance to personnel (Harrison, 2004). Previous studies on several Malaysian Armed Forces (MAF) vehicles showed that the noise level inside the driver's cabin increases with increasing truck speed (Aziz *et al.*, 2014a).

The objective of this study is to explain a new method for determination of noise exposure in the driver's compartment of Malaysian Army (MA) three-tonne trucks based on changing truck speed using the statistical analysis method known as Integrated Kurtosis-based Algorithm for *Z*-notch filter (I-kaz^{TM}). The findings of this study will demonstrate that I-kaz^{TM} is capable of providing noise exposure observation

2. INTEGRATED KURTOSIS-BASED ALGORITHM FOR Z-NOTCH FILTER (I-KAZ^{TM})

Statistical analysis is a mathematical science pertaining to the collection, analysis, explanation and determination the distribution of data and classification of random signals. In this study, statistical analysis for noise exposure was performed using the I-kaz^{TM} method, which was developed to detect changes in measured mechanical signals. I-kaz^{TM} was developed for both descriptive and inferential statistics, whereby the numerical descriptor of I-kaz^{TM} is the I-kaz^{TM} coefficient Z^{∞}. This is supported by 3D graphical summarisations of the frequency distribution known as the I-kaz^{TM} display. It is used to model patterns in the data, accounting for randomness and drawing inferences about the larger population, which is classified as the inferential statistics. Unlike existing statistical analyses, such as standard deviation, variance and kurtosis, this method can indicate both amplitude and frequency differences by simultaneously obtaining Z^{∞} and the I -kaz^{TM} 3D display (Nuawi et al. 2008).

The main idea of the I-kaz^{TM} method is decompose a time domain signal into three frequency ranges, which are low-frequency (LF) range of 0–0.25 f_{max}, high-frequency (HF) range of 0.25 f_{max} –0.5 f_{max} and very high-frequency (VF) range of 0.5 f_{max}. The selection of 0.25 f_{max} and 0.5 f_{max} as the low and high frequency limit respectively was chosen by considering the 2nd order of the Daubechies concept in the signal decomposition process (Daubechies 1992). Z^{∞}, as shown in the following equation, measures the space of scattering in the I-kaz^{TM} display:

$$Z^{\infty} = \sqrt{\frac{\sum_{i=1}^{N}(x_i^L-\mu_L)^4}{N^2} + \frac{\sum_{i=1}^{N}(x_i^H-\mu_H)^4}{N^2} + \frac{\sum_{i=1}^{N}(x_i^V-\mu_V)^4}{N^2}} \quad (1)$$

where x_i^L, $x_{i,}^H$ and x_i^V are the values of discrete data in the LF, HF and VF ranges respectively, at the i^{th} sample of time; μ_L, μ_H and μ_V are the means of each frequency band; and N is the number of samples.

I-kaz^{TM} was used for extracting the raw data features of sound pressure P that was measured from the sound level meter during noise monitoring. The recorded data was transferred to a computer, and analysed using MATLAB to compute Z^{∞} and produce the I-kaz^{TM} display in real time (Aziz *et al.* 2014b).

3. METHODOLOGY

This study was conducted on a Malaysian highway with tarmac road surface. A DuO smart noise monitor that utilises an A-weighted scale was used to measure *P* in the truck driver's compartment, with its calibration performed using a Bruel & Kjaer 4231 calibrator. The measurements were conducted at various truck speeds (0, 40, 80 and 100 kmh^{-1}), and were done at the same level as the ear position of the drivers as stated in ISO (1980) (Fig. 1).

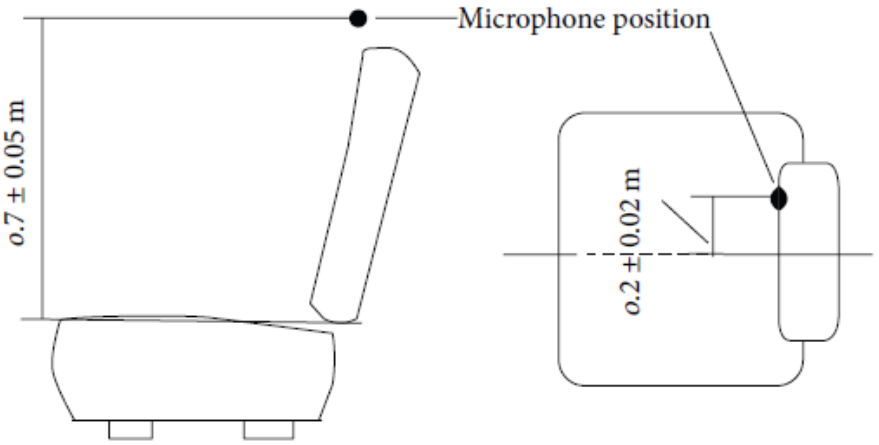


Figure 1: Microphone position at the driver's seat
Source: ISO (1980)

The measurement for each truck speed was repeated to ensure that the data is accurate and reliable for further analysis. All the measured raw data was converted to sound pressure level (SPL) in dB(A) using the following equation:

$$SPL = 20 \log_{10} \frac{P}{P_{ref}} \quad (2)$$

where P_{ref} is the reference sound pressure value of 20 $x10^{-6}$ Pa. The arithmetic mean value for each trial was determined. The measurements were considered as valid if the range of the measurements at each speed made immediately one after the other was not greater than 2 dB(A) (Aziz *et al.*, 2014b). The highest *SPL* value given by these measurements constituted the result (MNRE, 1987) and was used as raw data for the I-kaz™ statistical analysis.

4. RESULTS AND DISCUSSION

Table 1 shows the change of values of $\not{Z}^{\infty}$, *P* and *SPL* with varying truck speed. The truck at the idle position showed the lowest *SPL* (67.7 dB(A)) and $\not{Z}^{\infty}$ (3.39 x 10^{-8}) values. When the truck speed was increased, *SPL* and $\not{Z}^{\infty}$ also increased proportionately, with the highest truck speed (100 kmh^{-1}) showing the highest *SPL* (82.4 dB(A)) and $\not{Z}^{\infty}$ (1.04 x 10^{-6}). Previous studies on several numbers of Malaysian Armed Forces (MAF) vehicles also indicated that noise and vibration levels increased with increasing vehicle speed (Aziz *et al*., 2012, 2014). When the truck is moving at increasing speed, the noise and vibration produced from the engine, exhaust, road-tyre interaction, rear cabin and others increase.

Table 1: Values of P, $\not{Z}^{\infty}$ and SPL for the various speeds of the truck.

No. of test	Truck speed (kmh^{-1})	$\not{Z}^{\infty}$	P (Pa)	SPL (dB(A))	SPL_{avg} (dB(A))
1	0	2.85×10^{-7}	0.0570	69.1	68.1
2		7.17×10^{-8}	0.0480	67.6	
3		3.39×10^{-8}	0.0485	67.7	
4	40	6.93×10^{-7}	0.1026	74.2	73.7
5		8.62×10^{-7}	0.0925	73.3	
6		5.08×10^{-7}	0.0968	73.7	
7	80	1.15×10^{-6}	0.1722	78.7	79.1
8		5.46×10^{-7}	0.1762	78.9	
9		8.75×10^{-7}	0.1954	79.8	
10	100	1.17×10^{-6}	0.2489	81.9	82.2
11		1.04×10^{-6}	0.2637	82.4	

Figure 2 shows the I-kaz™ displays for the various truck speeds. From the data dispersion, it can be concluded that the lower value of $\not{Z}^{\infty}$ at 0 kmh^{-1} represents small space scattering, while its higher value at 100 kmh^{-1} represents larger space scattering. This method is used to model the data patterns from the I-kaz™ display, which accounts for the randomness and draws inferences from a larger population. It is developed based on the concept of data scattering about the data centroid and classifies the display according to inferential statistics. The I-kaz™ method is used to model the data patterns, which accounts for the randomness and draws inferences from a larger population. These inferences are very useful for estimating and forecasting future observations (Nuawi *et al*. 2009). This indicates that increase of *SPL* will result in increase of data scattering in the I-kaz™ display and value of $\not{Z}^{\infty}$.

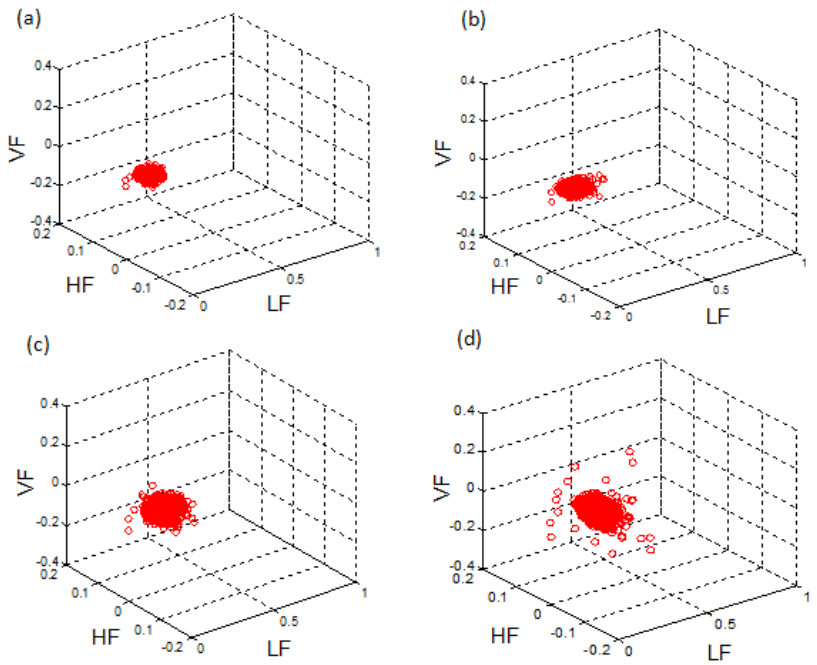


Figure 2: I-kaz™ displays for truck speeds of: (a) 0 kmh^{-1}, $\not{Z}^{\infty} = 2.85 \times 10^{-7}$ (b) 40 kmh^{-1}, $\not{Z}^{\infty} = 6.93 \times 10^{-7}$ (c) 80 kmh^{-1}, $\not{Z}^{\infty} = 8.75 \times 10^{-7}$ (d) 100 kmh^{-1}, $\not{Z}^{\infty} = 1.04 \times 10^{-6}$.

5. CONCLUSION

In this paper, noise exposure for MA three-tonne truck drivers was analysed using the I-kaz^{TM} statistical analysis method. The study showed that Z^{∞} increased proportionately with increasing *SPL*. From the I-kaz^{TM} displays, there was increasing size of data scattering for increasing SPL and truck speed. The I-kaz^{TM} displays are capable of providing noise exposure observation, because it can detect small changes of noise exposure. Thus, a warning system of excessive noise exposure, particularly for comfort and health of MA three-tonne truck drivers, can be developed using the statistical analysis method proposed in this paper.

ACKNOWLEDGEMENT

This paper was presented as a poster presentation during the 11th International Congress on Noise as a Public Health Problem (ICBEN 2014), which was held in Nara, Japan on 1-5 June 2014.

REFERENCES

Aziz, S.A.A., Nuawi, M.Z., Nor, M.J.M., & Daruis, D.D.I. (2014a). Study of Noise, Vibration and Harshness (NVH) for Malaysian Army (MA) 3-Tonne Trucks. *Appl. Mech. Mater.*, **471**: 74–80.

Aziz, S.A.A., Nuawi, M.Z., Nor, M.J.M., & Daruis, D.D.I. (2014b). New regression models for predicting noise exposure in the driver ' s compartment of Malaysian Army three-tonne trucks. *Adv. Mech. Eng.*, Art. ID 616093.

Bernama (2011). *More Armed Forces Staff Have Hearing Problems.* Bernama article dated 26 January 2011.

DHHS (U.S. Department of Health and Human Services) (1998). *Occupational Noise Exposure*. Department of Health and Human Services, U.S.

DOD (U.S. Department of Defense) (1991). *MIL-STD-1474C: Noise Limits for Military Materiel.* U.S. Army Research Laboratory, Department of Defense (DOD), U.S.

DOD (U.S. Department of Defense) (1993). *MIL-HDBK-767(MI): Design Guidance for Interior Noise Reduction In Light-Armored Tracked Vehicles*. U.S. Army Research Laboratory, Department of Defense (DOD), U.S.

Fooladi, M.M. (2012). Involuntary and persistent environmental noise influences health and hearing in Beirut, Lebanon. *J. Environ. Public Health*, Art. ID 235618.

Harrison, M. (2004). *Vehicle Refinement: Controlling Noise and Vibration in Road Vehicles*. Butterworth-Heinemann, Oxford.

Humes, L.E., Joellenbeck, L.M., & Durch, J.S. (2006). *Noise and Military Service: Implications for Hearing Loss and Tinnitus.* National Academies Press, Washington, DC.

ISO (International Organization for Standardization) (1980). ISO 5128: *Acoustics – Measurement of Noise Inside Motor Vehicles.* International Organization for Standardization (ISO), Geneva.

MNRE (Ministry of Natural Resources and Environment) (1987). *Environmental Quality Act 1974 - Federal Subsidiary Legislation: Environmental Quality (Motor Vehicle Noise) Regulations 1987*. Department of Environment, Ministry of Natural Resources and Environment (MNRE), Malaysia.

Nakashima, A.M., Borland, M.J. & Abel, S.M. (2007). Measurement of noise and vibration in Canadian Forces Armoured vehicles. *Ind. Health*, **45**: 318–327.

Nuawi, M.Z., Nor, M.J.M., Jamaludin, N., Abdullah, S., Lamin, F., & Nizwan, C.K.E. (2008). Development of Integrated Kurtosis-Based Algorithm for Z-Filter technique. *J. Appl. Sci.*, **8**: 1541–1547.

Pääkkönen, R. & Lehtomäki, K. (2005). Protection efficiency of hearing protectors against military noise from handheld weapons and vehicles. *Noise Health*, 7: 11–20.

Weatherless, R. A., Fedele, P. D., Kehring, K. L., & Letowski, T. R. (2012). The effects of simulated hearing loss on speech recognition and walking navigation. *Hum. Factors*, **55**: 285–297.

TREND ANALYSIS AND FORECASTING OF RAINFALL AND FLOODS IN THE KLANG VALLEY

Nor Hafizah Mohamed[1], Aminah Ismail[2], Zaulin Ismail[3], Che Wan Muhd Salleh Wan Adnan[3] & Mohd Faizal Abd Raji[3]

[1]Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence Malaysia, Malaysia
[2]Malaysian Meteorological Department (MMD), Ministry of Science, Tehnology & Innovation, Malaysia
[3]National Institute of Public Administration (INTAN), Malaysia

ABSTRACT

The purpose of this study is to determine the trend of amount of rainfall and number of flood incidents in the Klang Valley for the period of January 2008 to June 2013 for forecasting. The study was conducted using three analysis techniques, which were trend, time series and regression analyses. The results of the trend analysis showed that there was no significant trend in the graphs of rainfall and floods. Of the time series models used, the exponential smoothing model was found to have the lowest mean absolute value deviation (MAD) from the actual meteorological data and hence, was selected as the best forecasting model. Based on this model, the predicted values for Q3, 2013 in the Klang Valley for amount of rainfall and number of flood incidents were 4,103.24 mm and three respectively. Based on the results of the regression analysis, the correlation coefficient showed a weak relationship between the amount of rainfall and number of flood incidents. The results of the statistical analysis demonstrated that there is not enough evidence to indicate that there is a significant relationship between the two parameters.

Keywords: *Amount of rainfall; number of flood incidents; trend analysis; time series analysis; regression analysis.*

1. INTRODUCTION

Malaysia has a climate that is categorised as equatorial, as it is located near the equator. Being hot and humid all year round, its average rainfall is around 250 cm a year, while the average temperature is 27 °C. Malaysia experiences two monsoon seasons, the Southwest Monsoon from late May to September, and the Northeast Monsoon from November to March. The Northeast Monsoon usually brings in more rainfall as compared to the Southwest Monsoon, originating from China and the north Pacific. The transition period of the two monsoons is between March and October (MMD, 2014).

In recent years, natural disasters due to rain, especially floods and landslides, have often occurred in Malaysia, resulting in loss of lives and damage to properties. For example, the floods that occurred in Peninsular Malaysia from 30 October 2010 to 11 November 2010, and from 30 January 2011 to 15 February 2011 resulted in a total of 231,337 victims from 57,094 families being relocated to 906 evacuation centres and 21 people dead. In the past decade, the country has experienced several major floods. Across flooded areas of about 29,000 km^2, or 9% of the area of the country, more than 2.7 mil. people were affected. The total flood damage was assessed to be more than RM 100 mil. (NSC, 2011). According to the President of the Malaysian Society for Engineering and Technology (mSET), Dato' Prof. Dr. Abang Abdullah Abang Ali, the current situation is even more worrying because according to the statistics released by the Malaysian Meteorological Department (MMD), it is found that Malaysians are increasingly at risk of natural disasters due to abrupt climate changes, such as rising rates of rainfall, thunderstorms and landslides (Bernama, 2013).

Therefore, accurate prediction of rainfall is very useful for managing the preparation for the possibility of floods. It would also facilitate the MMD in issuing early warnings to local residents. According Rozilawati (2001), forecasting of rainfall in Malaysia as a whole is done manually by

several forecasters, with no one single model or formula used. This has caused difficulty to the MMD in providing accurate predictions. Inaccurate forecasts can increase the risk of loss of lives and damage to properties, in addition to making the preparation for disaster planning by the authorities more difficult. While the MMD has developed a predictive rainfall modelling system, it still needs to be improved (MMD, 2014).

Precipitation is one of the processes or reactions for multiple earth systems, including flood plain systems, to achieve stability. The magnitude of the influence rainfall on a particular system depends largely on the intensity of rainfall over a period of time (Moody & Deborah, 2001; Daniel *et al*., 2006; Azumi *et al*., 2010; Muhammad Barzani *et al*., 2010). Siti Fadzilatulhusni and Main (2011) found that there is a very close relationship between floods, and rapid development and urbanisation. If development processes are not done in a sustainable approach, it would result in higher likelihood of severe floods. Most of the researches conducted in regards to rainfall forecasting have used satellite information data or single station meteorological data. Liu & Lee (1999) suggested that datasets from multiple meteorological stations should be used to form a better understanding of the rainfall characteristics of an area. There have also been numerous researches conducted using neural networks, such as by Liu & Lee (1999), McCullagh *et al*. (1999) and Luk *et al*. (2000). For the purpose of flood forecasting and river monitoring in the Klang Valley, the Department of Irrigation & Drainage (DID) has developed the Integrated Flood Forecasting and River Monitoring System (IFFRM) (Livia *et al*., 2012). It can be concluded that there have been numerous extensive researches conducted in the area of rainfall and flood forecasting and trend analysis. However, as the world's climate condition continues to change year by year, the need for continuous and localised monitoring and research will always be highlighted as crucial.

The purpose of this study is to determine the trend of amount of rainfall and number of flood incidents in the Klang Valley for the period of January 2008 to June 2013 for forecasting. The main objectives of this research are:

i. To compare the trends of amount of rainfall and number of flood incidents.
ii. To forecast the amount of rainfall and number of flood incidents that would occur in the third quarter (July-September) of 2013. This would then be compared with the actual meteorological data for verification.
iii. To determine the relationship between the amount of rainfall and number of flood incidents that occurred.

2. METHODOLOGY

2.1 Data Collection

This study required data on rainfall and floods in the Klang Valley for the period of January 2008 to June 2013. Rainfall data was obtained from six meteorological stations in the Klang Valley, which were KLIA Sepang, Petaling Jaya, Subang, Ampangan Ulu Langat, JAKOA Gombak and Klang Gate, while flood data was obtained from the DID. The data was sorted on a quarterly basis and plotted against time (Figure 1). It should be noted that this study did not include other meteorological data, such as mean sea level pressure, temperature, wind speed and direction, and seasonal climates, which may affect the forecast results.

2.2 Data Analysis

The study was conducted using three analysis techniques, which were trend, time series and regression analyses. The analyses adopted the Excel and Excel QM software in order to obtain the results.

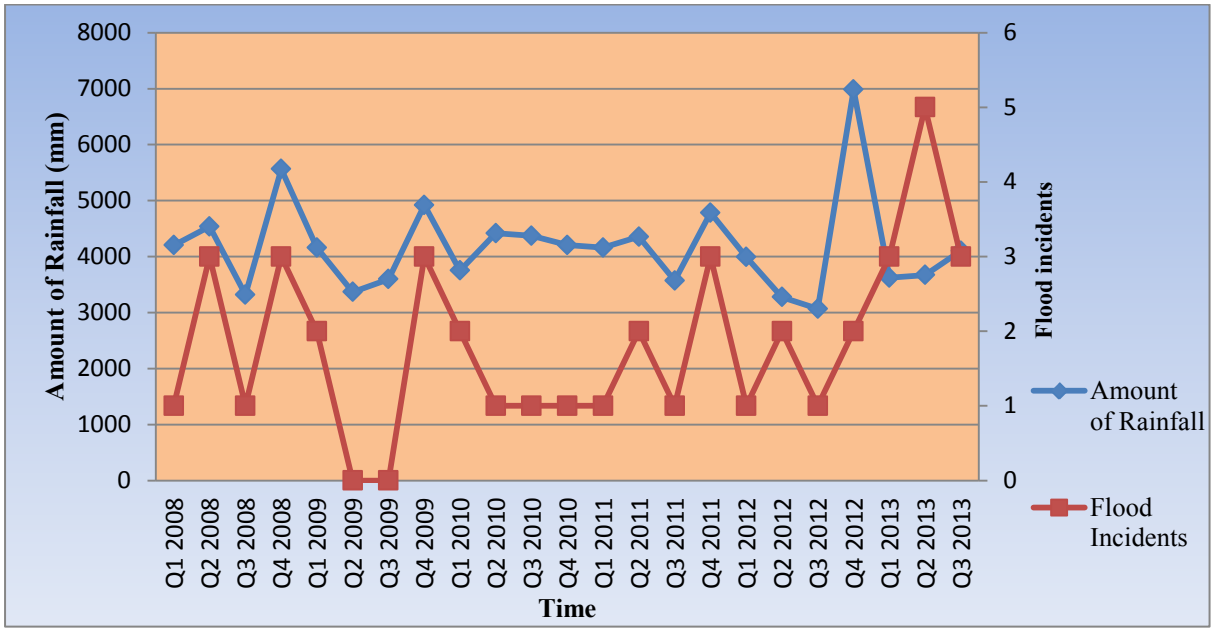


Figure 1: Collected data on amount of rainfall and number of flood incidents in the Klang Valley.

2.2.1 Trend Analysis

In order to determine the trends of amount of rainfall and number of flood incidents, trend analysis was used. It was performed through upward or downward movement of the data over time with a linear or curve-linear (non-linear) trend. Typically, the curve would be projected into the future for medium and long-term forecasts. There are several mathematical trend equations that can be developed, such linear, exponential or quadratic equations. In other words, the mathematical trend equation that would be developed would be a straight line that describes the relationship between the variables to be predicted (total amount of rainfall and number of flood incidents) and the variable used in the prediction (time or period) (Render and Stair, 2012).

2.2.2 Time Series Analysis

Time series models are used to predict future behaviour using historical data. These models make the assumption that what has happened in the past is an indicator on what will happen in the future. In other words, time series models refer to what has happened over a period of time and use a series of past data to conduct a forecast (Render and Stair, 2012). This study used time series analysis with three types of models to predict the amount of rainfall and number of flood incidents for Q3, 2013 (July-September):

i. **Naïve model**:
This model makes the assumption that the present is the best predictor of the future. A simple example of a naive model type would be to use the actual value of the current period as the forecast for the next period. In this study, Q2 2013 is the period would be used to forecast Q3 2013.

ii. **Exponential smoothing model**:
Both moving averages and weighted moving averages are effective in smoothing out sudden fluctuations in the demand pattern in order to provide stable estimates. In fact, increasing the size of *k* (number of periods averaged) smoothes out fluctuations even better. However, doing so requires extensive records of past data. An alternative forecasting approach that is also a type of moving average technique, but requires little record keeping of past data, is called exponential smoothing. This model uses smoothing constant of time series models for predictions. A smoothing constant where α is a weight that has a value between 0 and 1. The smoothing constant can be changed to give more weight to recent data when the value is high

or more to past data when it is low. For this study would be used the smoothing constant value, α is 0.4, it can be shown mathematically that the new forecast is based almost entirely on value in the past periods..

iii. **Moving average model**:
Moving averages are useful if we can assume the item we are trying to forecast will stay fairly steady over time. We calculated a two-period moving average by summing the actual value of the item for the past two periods and dividing the total by 2. This moving average serves as the forecast for the next period. With each passing period, the most recent period's actual value is added to the sum of the previous two periods' data, and the earliest period is dropped. This tends to smooth out short-term irregularities in the time series. For this study, the two previous quarters (Q1 and Q2, 2013) were used for prediction of Q3, 2013.

The overall accuracies of the forecasting models were determined based on the mean absolute value deviation (MAD) from the actual meteorological data. The model with the lowest value of MAD was determined as the best model for prediction of the amount of rainfall and number of flood incidents.

2.2.3 Regression Analysis

Regression analysis is the analysis of the linear relationship between two or more independent variables and the dependent variable. This analysis is used to determine the direction of the relationship between independent variables with dependent variables which relate either positively or negatively, and to determine the value of the dependent variable when the independent variables show an increase or decrease. In this study, regression analysis was used to determine if there is a significant relationship between the amount of rainfall *X* and number of flood incidents *Y*, which were the independent and dependent variables respectively. The regression equation can be described as follows (Piaw, 2012):

$$Y = a + bX + e \quad (1)$$

where:

a: Constant (*Y* when *X* = 0)
b: Regression coefficient
e: Error / residual.

3. RESULTS & DISCUSSION

3.1 Trend Analysis

Through observations made for the period of January 2008 to June 2013 (Figure 1), there were patterns of similarities between the amount of rainfall and number of flood incidents, whereby increase in amount of rainfall showed increase in number of flood incidents. While patterns of similarities were observed between the two datasets, no significant trend was observed.

The amount of rainfall from Q1, 2010 to Q1, 2011 showed no significant difference; there were no quarterly fluctuations as was the case in the other quarters, and it appeared to be distributed evenly throughout the period. This might be caused by weather phenomenon, such as La-Nina, which can affect the amount of rainfall. The number of flood incidents also showed a similar pattern. In Q2, 2013, it was also observed that although the amount of rainfall decreased, the number of flood incidents increased. It is likely that this quarter, covering the months of April, May and June, marks the transition monsoon, where convective rain often occurs, causing high intensity of rainfall in a short period. This can be seen by the amount of rainfall measured hourly.

Trend analysis for both datasets was done against time, with the results shown in Figure 2. From the trend analysis, the amount of rainfall for Q3, 2013 in the Klang Valley was predicted to be 4143.8 mm while the number of flood incidents was predicted to be two.

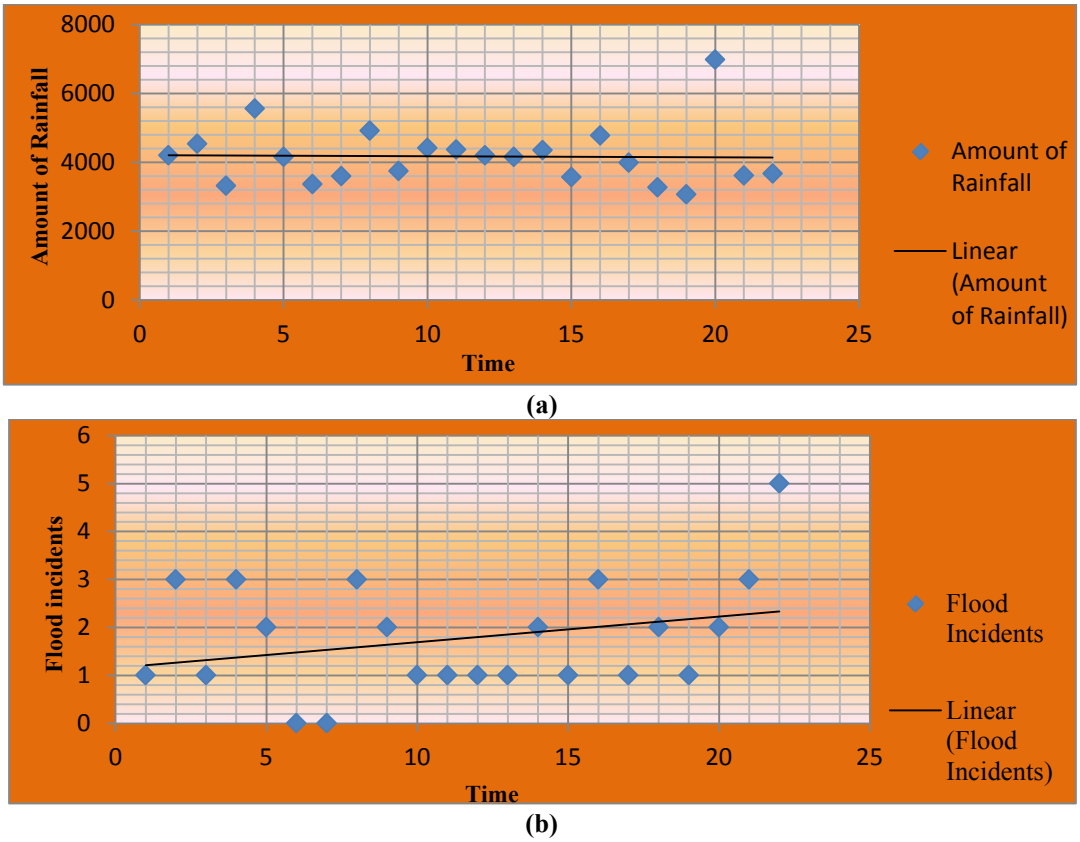
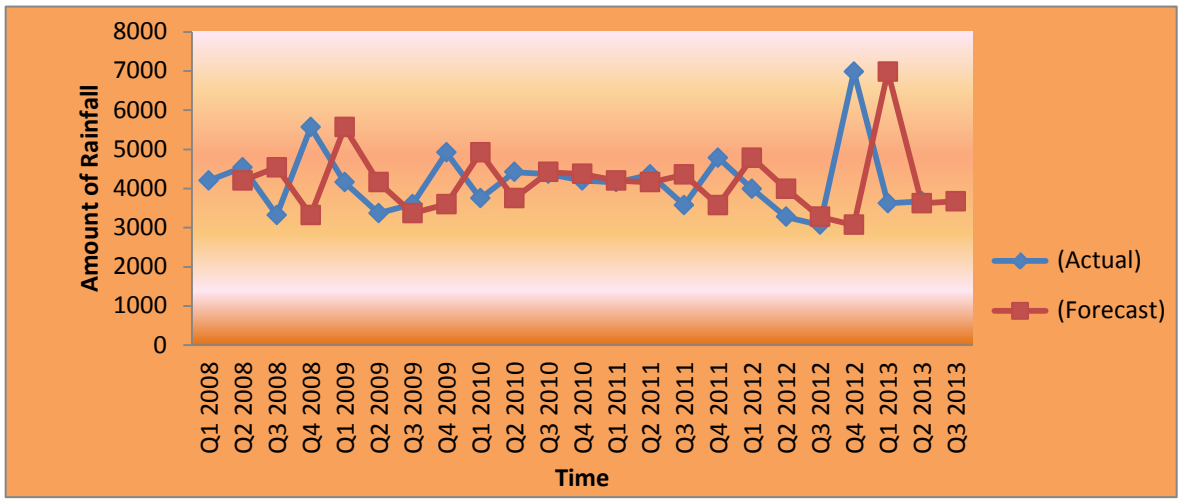


Figure 2: Trends of (a) amount of rainfall and (b) number of flood incidents against time.

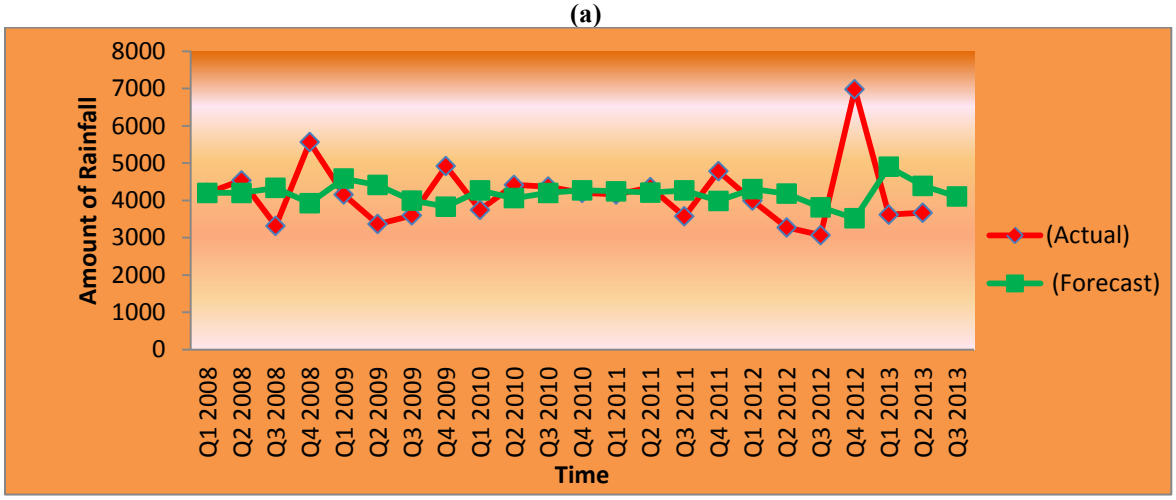
3.2 Time Series Analysis

Comparisons of actual and forecast graphs for the Naïve, exponential smoothing and moving average models are shown in Figures 3 and 4, for amount of rainfall and number of flood incidents respectively. For all the plots, it is observed that that the differences of scattering data between the actual and forecast graphs are small, indicating that the predicted data is highly accurate and almost similar to the actual data.

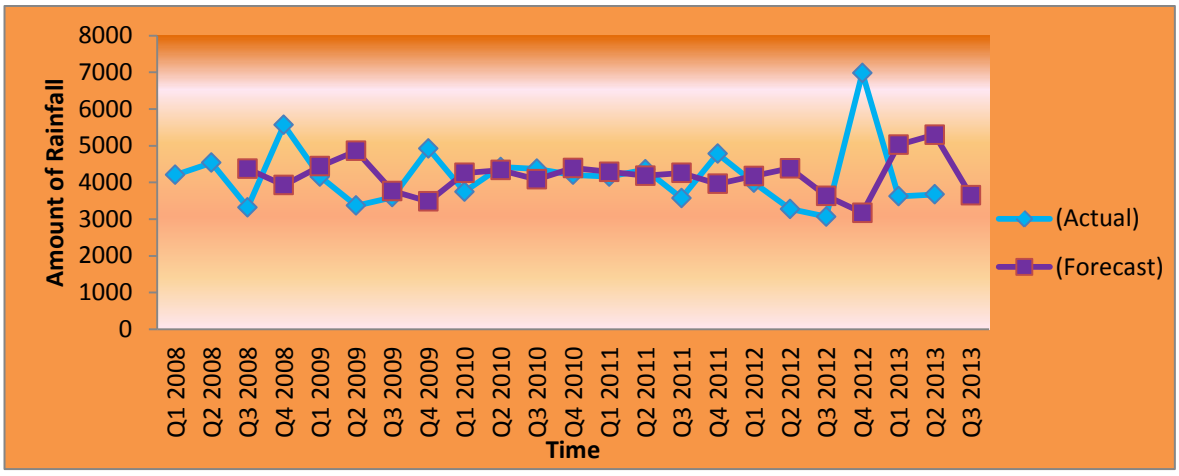
As shown in Table 1, the exponential smoothing model has the lowest MAD values for both amount of rainfall and number of flood incidents, and hence, was selected as the best forecasting model. Based on this model, the predicted values for Q3, 2013 in the Klang Valley for amount of rainfall and number of flood incidents are 4,103.24 mm and three respectively.



(a)

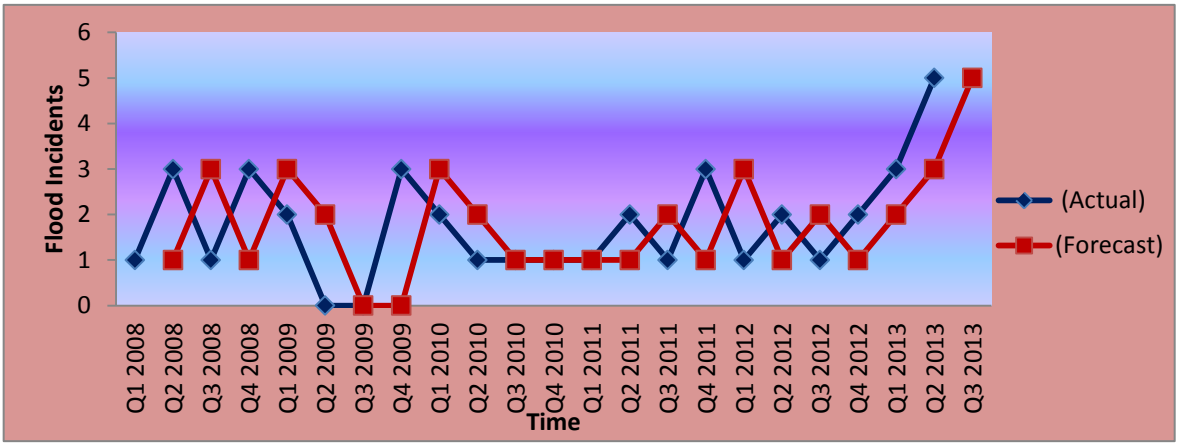


(b)

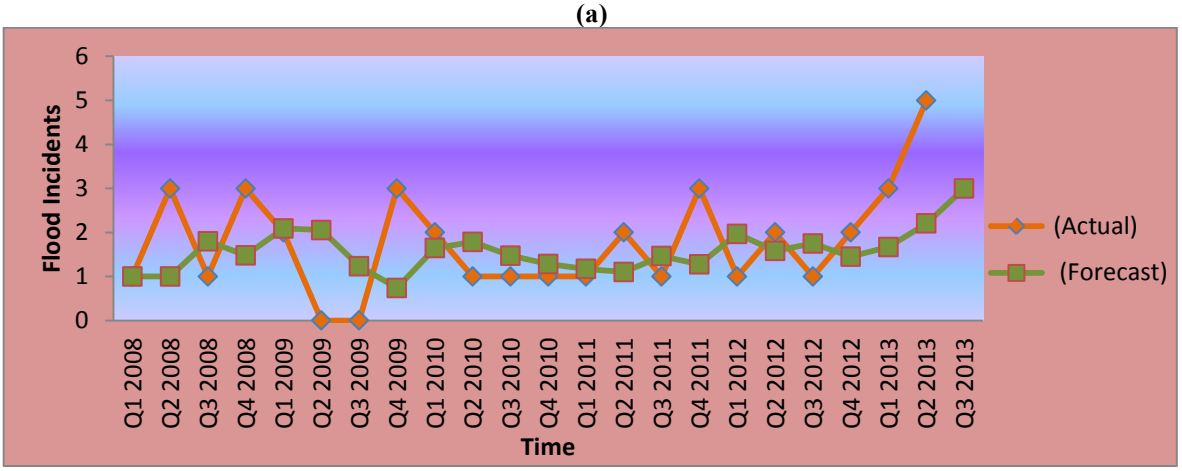


(c)

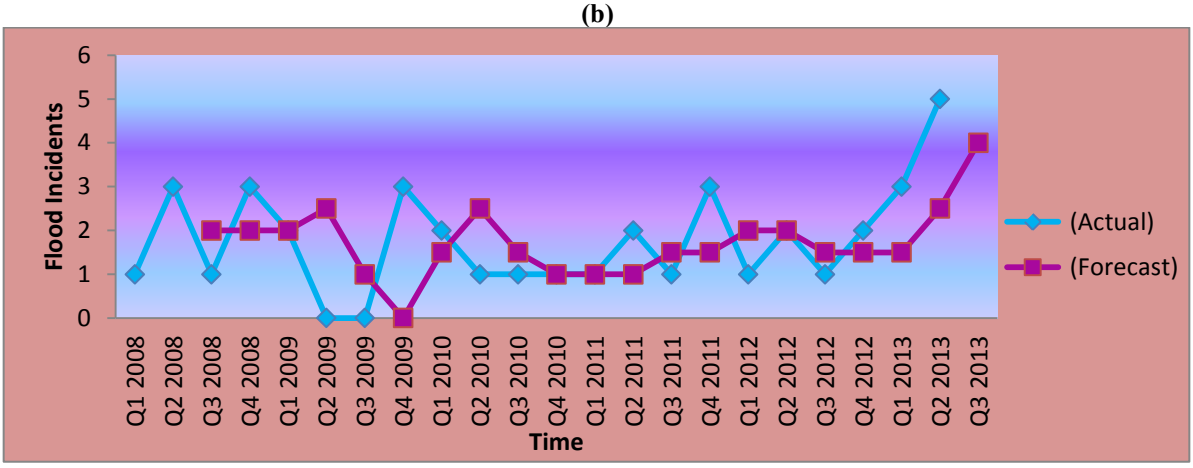
Figure 3: Comparison of actual and forecast data for amount of rainfall for the (a) Naïve, (b) exponential smoothing and (c) moving average models.



(a)



(b)



(c)

Figure 4: Comparison of actual and forecast data for number of flood incident for the (a) Naïve, (b) exponential smoothing and (c) moving average models.

Table 1: Predicted and MAD values for the forecasting models.

Parameter	Model	Predicted value	MAD
Amount of rainfall (mm)	Naïve	3, 671.90	993.88
	Exponential smoothing	4,103.24	736.52
	Moving average	3,646.45	882.41
Number of flood incidents	Naïve	5	1.24
	Exponential smoothing	3	0.99
	Moving average	4	1.00

3.3 Regression Analysis

Regression analysis was used to determine if the relationship between the amount of rainfall and number of flood incidents is significant, based on the following hypothesis:

H_o: There is no linear relationship between the amount of rainfall and number of flood incidents.
H_a: There is a linear relationship between the amount of rainfall and number of flood incidents.

Based on the computed regression statistics in Table 2, the correlation coefficient r is 0.2835, indicating that the relationship between the amount of rainfall and number of flood incidents is weak. The value for coefficient of determination R^2 is 0.0804, indicating that there was only 8% change in the number of flood incidents in the Klang Valley was due to the amount of rainfall recorded.

Table 2: Regression statistics for the relationship between the amount of rainfall and number of flood incidents.

Parameter	Value
Correlation coefficient *r*	0.2835
Coefficient of determination R^2	0.0804
Error *e*	1.1895
Observations	21

Based on analysis of variance (ANOVA, Table 3), at 95% confidence level, the value of p (0.2129)> α (0.05) provided enough evidence to accept H_o. Therefore, statistically, there is no linear relationship between the amount of rainfall and number of flood incidents. From the analysis carried out, the amount of rainfall does not influence the number of flood incidents in the Klang Valley. This is because the flood data was obtained in the form of flood frequency instead of flooding period (number of days of flooding).

Table 3: Analysis of variance (ANOVA) for the relationship between the amount of rainfall and number of flood incidents.

Parameter	Degree of Freedom *df*	Sum of Square *SS*	Mean Square *MS*	*F*-Ratio	Value of *p* (Significance of *F*)
Regression	1	2.351374	2.351374	1.66164203	0.212855576
Residual	19	26.88672	1.415091		
Total	20	29.2381			

4. CONCLUSION

This study dealt with the determination of trends, relationships and forecasts of rainfall and floodings. The results of the trend analysis showed that there was no significant trend in the graphs of rainfall and floods. Of the time series models used, the exponential smoothing model was found to have the lowest MAD from the actual meteorological data and hence, was selected as the best forecasting model. Based on this model, the predicted values for Q3, 2013 in the Klang Valley for amount of rainfall and number of flood incidents are 4,103.24 mm and three respectively. Based on the results of the regression analysis, the correlation coefficient showed a weak relationship between the amount of rainfall and number of flood incidents. The results of the statistical analysis demonstrated that there is not enough evidence to indicate that there is a significant relationship between the two parameters. The results of this study can be applied by various relevant agencies to assist in the implementation of socio-economic development planning and making the necessary disaster mitigations planning for the minimisation of loss of life and damage to property.

The results obtained show that floods are not just influenced by the amount of rainfall. Instead, floods are also affected by other factors, such as tidal rivers, the El Nino phenomenon, temperature, altitude, drainage and terrain. Therefore, further studies should be conducted to examine the influence of other factors on flood trends. A suitable model can be generated by using all the factors found to be relevant.

In order to improve this study, more data should be obtained to ensure that the results would be more accurate. This includes the addition of data from several more meteorological stations in the Klang Valley in order to represent every district in the territory, extracting more frequent rainfall data, such as hourly rainfall, and obtaining more comprehensive flood information, such as the number of days and areas affected by floods.

ACKNOWLEDGEMENT

The authors express utmost gratitude to Assoc. Prof. Dr. Zulkifli Mohd Nopiah for his support and advice especially in the operational research approach. The authors also gratefully acknowledge the cooperation and support given by the Malaysian Meteorological Department (MMD) and Department of Irrigation & Drainage (DID) for this research.

REFERENCES

Azumi SD, Supiah, S. & Azmi, A. (2010) Modelling the distribution of rainfall intensity using hourly data. *Am. J. Environmen. Sci.,* **6**: 238- 243.

Bernama. (2013). Flash flood havoc in KL. Available on line at: http://www.nst.com.my/latest/flash-flood-havoc-in-kl-1.252506 (Last access date: 26 April 2013).

Daniel L.C., Joseph N.B., Stephen E.D., Christoper J.M., David T.R. & Fred H.S. (2006). Relating precipitation and water management to nutrient concentrations in the Oligotrophic "upsidedown" estuaries of the Florida Everglades. *Limnol. Oceanogr*., **51**: 602- 616.

Liu, J.N.K. & Lee, R.S.T. (1999). *Rainfall Forecasting from Multiple Point Sources Using Neural Networks*. Hong Kong Polytechnic University, Hong Kong.

Livia, L., Abdul Razak, B. & Abdul Jalil, H. (2012). Intergrated Flood Forecasting and River Monitoring System (IFFRM). *Technical Session in Conjunction with MHS AGM*, 8 May 2012, DID Ampang, Kuala Lumpur.

Luk, K.C., Ball, J.E. & Sharma, A. (2001). An application of artificial neural networks for rainfall forecasting. *Math. Comput. Model.*, **33**: 683-693.

McCullagh, J., Bluff, K. & Hendtlass, T. (1999). Evolving expert neural networks for meteorological rainfall estimation. *Int. Conf. Neural Inform. Process. 1999*, 16-20 November, Perth.

MMD (Malaysian Meteorological Department) 2014. *Weather Forecast: Current Monsoon Report*. Available online at: http://www.met.gov.my (Last access date: 26 April 2014).

Moody J.A. & Deborah A.M. (2001). Post-fire, rainfall intensity-peak discharge relations for three mountainous watersheds in the Western USA. *Hydro. Process.* **15**: 2981- 2993.

Muhammad Barzani, G., Salmijah, S., Mazlin, M., Mohamad Ikhwan, T., Sahibin, A.R. & Chong, H.B. (2010). Analisis banjir Disember 2006: Tumpuan di kawasan Bandar Segamat, Johor. *Sains Malaysiana*, **39**: 353- 361.

NSC (National Security Council) (2011). *Kesiapsiagaan Bencana Semasa Monsun Timur Laut*. National Security Council (NSC), Prime Minister's Department, Malaysia.

Piaw, C.Y. (2012). *Kaedah dan Statistik Penyelidikan: Asas Statistik Penyelidikan (Buku 2)*. McGraw Hill (Malaysia) Sdn Bhd., Kuaka Lumpur.

Render, B. Jr.Ralph M.S. & Michael E.H.(2012). *Quantitative Analysis for Management. 7th Ed.* Pearson Education Limited, England.

Rozilawati, D. (2001). *Penggunaan Kaedah Statistik Di Dalam Pengelompokan Data Kajicuaca Bagi Meramal Taburan Hujan*. Universiti Teknologi Malaysia, Skudai, Johor.

Siti Fadzilatulhusni, M.S. & Main, R. (2011). *Analisis taburan hujan dan impaknya kepada sumber air di Pulau Pinang*. Malaysia Journal of Society and Space 7 issue 1(65 – 75), ISSN 2180-2491.

DESIGN OF A VIRTUAL HYBRID HONEYNET BASED ON LXC VIRTUALISATION FOR ENHANCED NETWORK SECURITY

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

Honeynet represents a theory in network protection. Unlike purely defensive methods, such as intrusion detection systems (IDS), data encryption and firewalls, that try to avoid interaction with the attacker, Honeynet is based on the idea of interaction with the attacker. During this interaction, Honeynet records all of the attacker's actions and tools used without the attacker knowing. This data is sent to security analysers to study and prepare defensive methods. Honeynet can also protect physical computers and infrastructure by duplicating them virtually and presenting this virtual environment instead of the real systems to any person trying to gain unauthorised access to the network. In this work, a hybrid Honeynet, including both the low- and high-interaction honeypots, was developed and implemented utilising virtualisation technology to represent a typical laboratory environment in University Putra Malaysia (UPM). Different virtualisation methods were evaluated based on their ability to deploy a stable Honeynet, with Linux containers (LXC) proving to be more efficient in deploying a large scale Honeynet as compared to other virtualisation methods.

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

1. INTRODUCTION

Traditionally, information security protection has primarily relied on defensive strategies such as data encryption, intrusion detection systems (IDS) and firewalls. This defensive strategy is based on the notion of detecting and enhancing the security of computer systems and networks before they interact with the others. As the hacker has the initiative, given that these systems rely on pre-set conditions and rules, they cannot protect the infrastructure as once the exploit is detected, the hacker can use it to gain access to the systems repeatedly until it is detected and fixed (Honeynet, 2014).

In order to overcome these limitations, researchers have developed a new method called Honeynet. In order to gather information about the tactics, tools and attack patterns used by the intruders, Honeynet interacts with the hacker by emulating real systems instead of presenting the physical systems. Security personnel can use the gathered information and intelligence data to enhance the weak points in the system against future hacking attempts. The goal of the Honeynet is to emulate a highly controlled network of computers and nodes where all the activities are monitored, controlled and captured. A Honeynet is made of many components such as data monitoring, control and capture, and honeypots act as the main component of the system (Figure 1) (Ligh *et al*., 2010; Kaur *et al*., 2012).

Since Honeynet does not add to the productivity of the network or system, it is better to minimise the effort of creating and maintaining them. Honeynet usually leverages on the enhancement offered by virtualisation technology to reduce the resource dependency. A scalable Honeynet based on virtual machines can offer great value in terms of ease of deployment and hardware utilisation (Ligh *et al*. 2010; Honeynet, 2014).

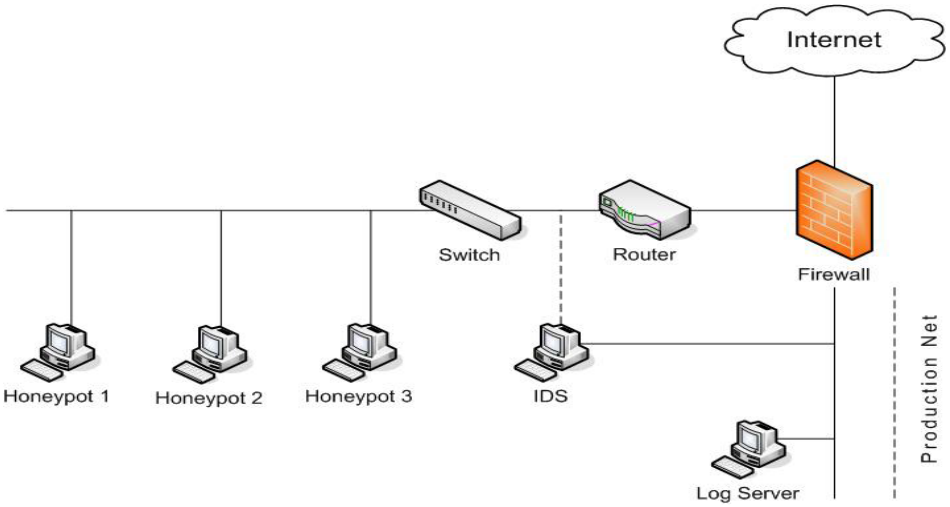


Figure 1: Design of a Honeynet.
(Source: Honeynet (2014))

In this paper, a virtual Honeynet is introduced. The proposed framework can handle large amounts of honeypots for deployment inside the Honeynet. The aims of study were designing a virtual Honeynet based on the typical layout of a lab in Universiti Putra Malaysia (UPM) and determining a proper virtualisation method by comparing the latest virtualisation methods while running the same Honeynet and configurations.

2. HONEYNET

2.1 Honeypots

Honeypots were introduced as an effective way for monitoring and interpreting the tactics and tools used by hackers. They can be considered as an evolution of Botnet idea (Konovalov *et al*., 2013). Honeypots can be defined as an information system resource that would be valuable when receiving illegitimate and unauthorised access (Provos & Holz, 2007). As the network administrators know the network addresses for all the honeypots, and as the honeypots usually do not interact with other systems, any network traffic on the Honeynet can potentially be a sign of malicious activity. All the data transmitted on the network associated with the honeypots are inspected and stored for further analysis, with the analysed data used to counteract future attempts to exploit the system. A wide variety of operating systems, services and ports can be simulated using honeypots (Nikkhahan *et al*., 2009; Ligh *et al*., 2010; Bao *et al*., 2010).

Based to their purpose and level of interaction, honeypots can be categorised to low- and high-interaction honeypots (Table 1) (Joshi & Sardana 2011). Low-interaction honeypots are based on the idea of presenting the intruder with an emulated but real looking system. This emulated system can be configured to control the allowed connections, emulated hardware, service and type of the operating system, thus defining the extent and the scope of the interaction with the intruder (Nikkhahan *et al*., 2009; Honeynet, 2014).

High-interaction honeypots are difficult to implement and require a good knowledge of data control and information security protocols. As these honeypots are full-fledged systems with high interaction with the outside world, care must be taken to prevent the falling of these systems to the intruder's control as they can be used as pawns to attack other systems both on and off site (Provos & Holz, 2007). The advantage of high interaction honeypots is that they can show the pattern that the attacker is taking to hack a system. As there are no emulated ports and / or internet protocol (IP) stacks, if the

intruder tries to open a closed port by any method, the tools and processes used are logged and captured for further analysis. These high-interactions providing security research data and gathering real time attack patterns which not gatherable by any other means (Nikkhahan *et al*., 2009; Honeynet, 2014).

Table 1: Comparison between low- and high-interaction honeypots. (Source: Joshi & Sardana, 2011)

Feature	Low-interaction	High-interaction
Degree of Interaction	Low	High
Real Operating System	No	Yes
Risk	Low	High
Knowledge to Gain Connections	Requests	Everything
Can be Conquered	No	Yes
Maintenance Time	Medium	Very High

2.2 Data Control in Honeynet

With a system like Honeynet, there is always the potential of a malicious code or intruder using it to harm or attack or non-Honeynet systems, or abusing the Honeynet in un-expected ways. Every possible effort must be taken to ensure that once a system is compromised or a hacker is within the Honeynet, it cannot harm other systems, purposefully or accidentally (Watson & Riden, 2008).

The challenge is minimising the chance of detection by the intruder after implementing data control. This is a complicated task and to ensure the maximum security, compromises have to be taken. The more activity that is allowed, the more information that can be potentially extracted about the attack pattern, and thus, the intruder must be given some degree of freedom to act. However, the more freedom that is given to the intruder, the more risks of the Honeynet being compromised and used to exploit other non-Honeynet systems. Based on the design requirements, Honeynet designers determine the balance of how much freedom to give the intruder versus how much to restrict their activity (Honeynet, 2014).

2.3 Data Capture and Analysis in Honeynet

Data capture is the monitoring and logging of all of the suspicious activities within the Honeynet. The tactics, tools, and motives of intruders are determined by analysing the captured data. In order to minimise the risk of failure while maximising the amount of data captured in case the system is compromised, in well implemented Honeynets, multiple layers of data capture are utilised (Joshi & Sardana, 2011). This modular layer based method ensures that the maximum amount of attacker activity is recorded even if there is a compromise or failure in any of the other data capture layers. This combination of layers helps piece together all of the intruder's actions. Care must be taken not to store the captured data inside the honeypots as this increases the risk of detection and deletion of the data by the intruder. In order to ensure reduced chance of detection, the modifications to the honeypots for data capture purposes must be kept at a minimum (Watson & Riden, 2008; Gani, 2012; Honeynet, 2014).

Data analysis is done based on the requirements of the organisation owning the Honeynet. Each organisation can choose what and how to analyse the captured data using the standard packet analyser of Honeynet in packet capture (pcap) format, called Honeywall analyser.

2.4 Virtualisation and Virtual Hybrid Honeynet

As acquiring and maintaining multiple powerful mainframe computers is not an option for many organisations, in order to provide resource sharing between users, IBM developed the concept of virtualisation and virtual machines. Virtualisation enables the running of multiple different operating systems and the use of multiple users within a single computer. This enables users and developers to evaluate their work on multiple isolated operating systems on the same computer without the worry of affecting the work or the data of other users on the same computer (Rose, 2004).

Virtual Honeynets refer to systems where the honeypots are stored and run from virtual machines. There are two main categories of virtual Honeynets capabilities (Avila, 2005; Chang & Tsai, 2010):

- Self-contained virtual Honeynet: The entire Honeynet network is implemented and executed from a single computer with the aid of a single virtual machine.
- Hybrid virtual Honeynet: The entire Honeynet network is implemented and executed from a single computer with the aid of separate virtual machines along with a separate physical computer for data control and added data capture capabilities (usually utilising a Honeywall) capabilities.

The kind of operating system installed on a machine depends on the type of the deployed Honeynet. A production Honeynet is limited to the preferences, components and software used in the real network which is being simulated, whereas for a research Honeynet, the preferences, components and software used can be chosen more freely. The machine running the virtualisation software is referred to as the "host" and each virtual machine represents a "guest". Virtual Honeynets have some key advantages over traditional Honeynets, such as ease of deployment and maintenance, ability to freeze the Honeynet state if required, and better memory, processor cycle and physical storage management (Provos & Holz 2007; Ligh *et al*., 2010; Honeynet, 2014).

3. MATERIALS AND METHODS

For this study, a hybrid virtual Honeynet was designed and implemented on a server mainframe running Linux Ubuntu 12.04 LTS over a Xenon processor and 4 GB of RAM. The data control and backup data capture was done using a separate physical computer utilising Honeywall (Provos & Holz, 2007), with bridged networking to avoid detection. It should be noted that while this computer has no network address, it captures all the data in the network. The designed Honeynet is a Hybrid type, combining both low- and high-interaction honeypots.

In order to achieve the required level of protection, Honeypots are placed behind special physical machine running the ROO software, also known as a Honeywall. The Honeywall acts as a transparent network bridge between the internal network or the Internet and the Honeynet. In order to reduce the risk of deploying a Honeynet, the Honeywall can do all the work of a traditional Honeynet namely data control, capture and analysis. This adds a second layer of security to the network in case of the Honeynet compromise. In this study latest version of ROO (version 1.4) software is used (Sharma & Sran, 2011; Honeywall, 2014).

The low interaction honeypots are configured by utilising Honeyd, which is a low interaction honeypot design tool that not only allows processes and hardware to be emulated, but also supports operating system emulation, thus representing the honeypot as close as possible to a physical computer system (Provos & Holz, 2007; Liu *et al*., 2011; Honeynet, 2014). In addition to its features, such as simulating many operating systems, it can also provide many TCP services like File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP) and Secure Sockets Layer (SSL) services. Honeyd can also be configured to emulate network properties

such as delay, packet loss rate and bandwidth (Kuwatly *et al*., 2004; Provos & Holz, 2007; Wang & Zeng, 2011). Figure 2 illustrates the architecture of Honeyd.

Honeyd emulates operating systems by responding with appropriate packets to incoming data connections just like dedicated physical systems. In order to increase hardware utilisation, and to increase the security and stability of the system in case of a compromised Honeynet by isolating it from the other Honeynets in the server, different virtualisation methods were used (Shinde, 2012). The LXC (LXC, 2014), Kernel-Based Virtual Machine (KVM) (Tang & Li, 2010; KVM, 2014), Virtual-Box (Virtual-Box, 2014) and VMware (VMware, 2014) virtualisation methods were tested based on their suitability to deploy a virtual Honeynet. Based on the results of the study, the LXC based virtualisation method was selected as it provided better performance.

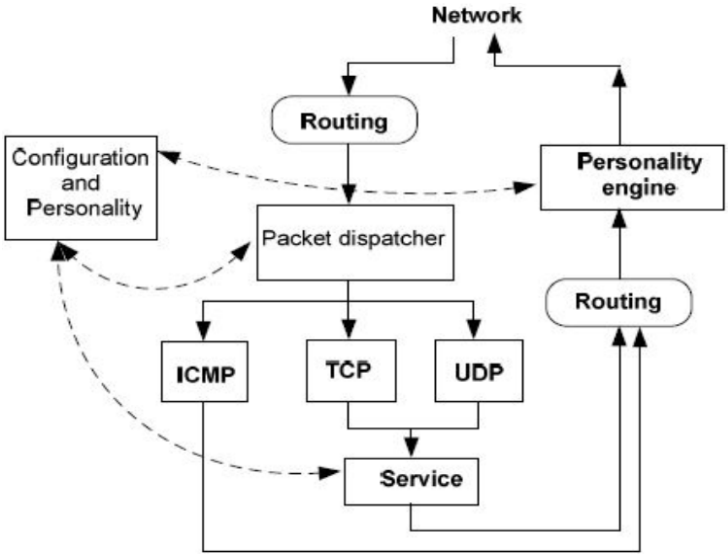


Figure 2: The architecture of Honeyd.
(Source: Provos & Holz (2007))

The design of the Honeynet is based on a combination of three different honeypots, each running Ubuntu 12.04 LTS on an isolated LXC virtual machine. Each of these honeypots represents a typical layout of a laboratory at UPM. Table 2 illustrates the number of services and operating systems emulated in each of the honeypots, referred to as Lab 1 to 3. In addition, a web server running Apache2 was added.

The high-interaction honeypot was based on online shopping as it is one of the most attacked websites on the internet. The web server was running a full online shopping system; it is configured as an electronics shop. Figure 3 shows the webserver, while Figure 4 illustrates the designed Honeynet.

Table 2: Operating systems emulated by the Honeypots.

Honeypot / Emulated OS	Lab 1	Lab 2	Lab 3
Windows 7	18	9	11
Windows XP	5	0	0
Windows Server 2008	1	1	0
Linux	0	12	0
Linux Server	0	1	0
Mac	0	0	4
Mac Server	0	0	1

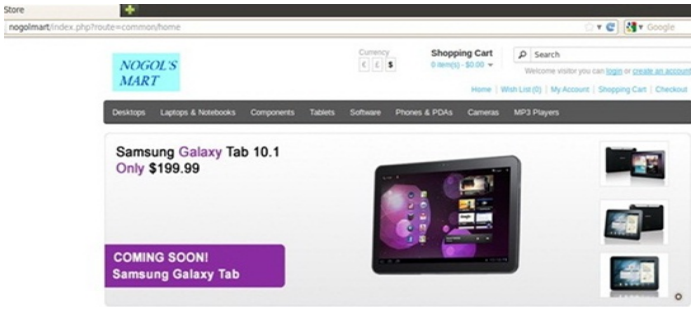


Figure 3: An example of an order page from the webserver of the Honeynet.

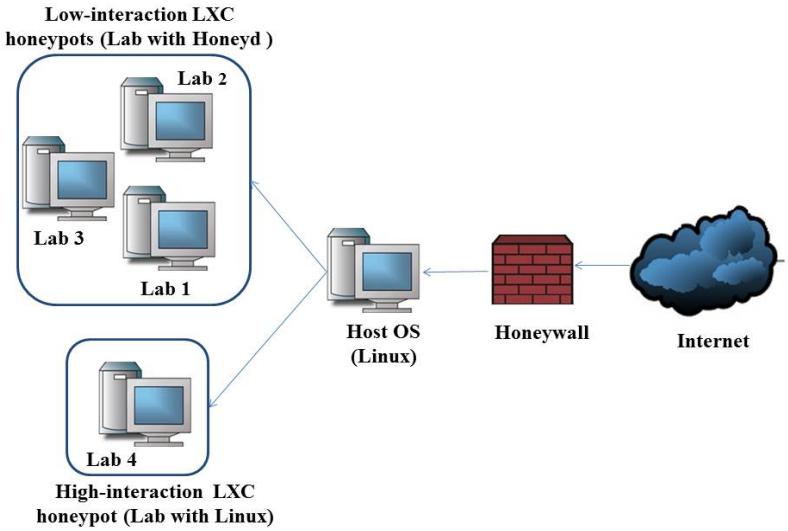


Figure 4: The architecture of the designed Honeynet.

4. RESULTS AND DISCUSSION

It was clear that LXC virtualisation was able to yield better results for implementing a Honeynet. Compared to the other virtualisation methods, VMware, VirtualBox and KVM, LXC virtualisation was able to provide better performance for implementing a Honeynet specifically while running multiple virtual machines simultaneously. Figure 5 shows the decrease in performance of the different virtualisation solutions while running a Honeynet simulating 1,000 Windows 7 systems as compared to the same Honeynet running on an identical operating system and parameters on the same hardware without any virtualisation.

Figure 6 shows the decrease in performance of the virtual machines while running multiple virtual machines simultaneously as compared to the instance of running just one virtual machine. While the decrease in performance in the case of VMware is noticeable, the other virtualisation methods managed to retain most of their performance figures.

In order to evaluate the Honeynet, Nmap (Nmap, 2014) was used to scan for open ports and to check whether the honeypot was replying to incoming data with appropriate response. The results of Nmap on one of the emulated Windows 7 systems indicated that it could detect a running operating system with 96% accuracy.

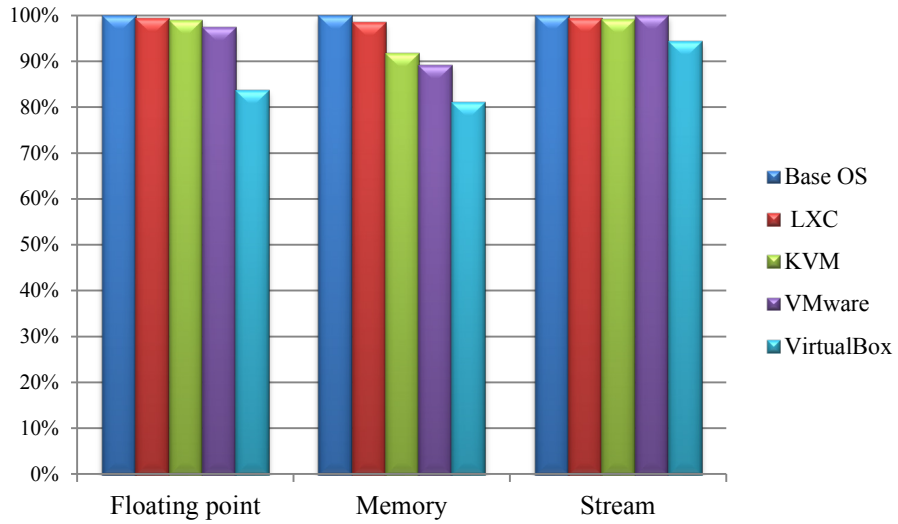


Figure 5: Decrease of the performance of different virtualisation solutions while running a Honeynet composed of 1,000 simulated Windows 7 systems.

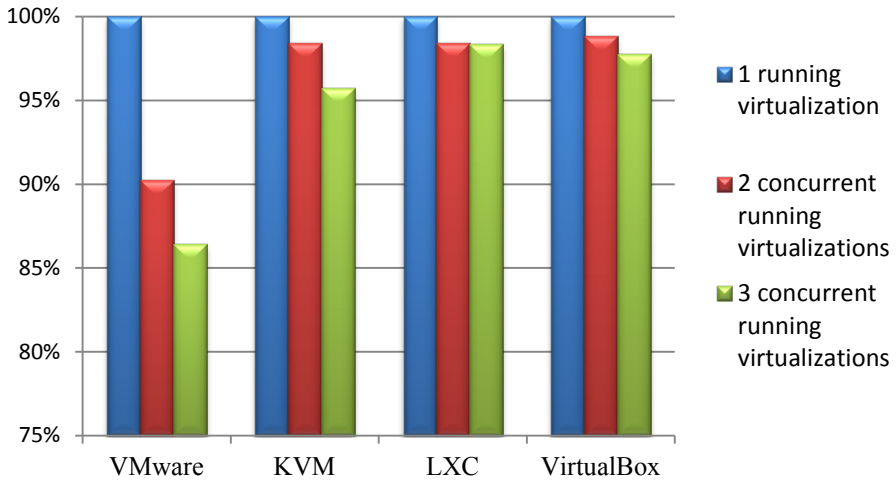


Figure 6: Decrease in performance of the host operating system while running multiple virtual machines simultaneously.

Although each of the Honeypots running in the LXC environment has the ability to capture and log the data and the requests forwarded to them, a secondary layer of data capture was added to increase the security of the Honeynet. This data capture was based on snort (Snort, 2014), which monitors all the data in and out the Honeynet, and reports any suspicious activities and alerts the user via email. Snort network monitoring and data control was created as an open-source and cross-platform network intrusion detection and prevention tool by Martin Roesch (Albin, 2011). It is based on real-time packet and network traffic analysis, such as detecting operating systems, stealth port scans, buffer overflows, fingerprinting attempts, server message block probes and common gateway interfaces. Snort uses a rule database tool identify suspicious activities on the network. These rules are constantly updated by the Sourcefire Vulnerability Research Team (VRT) on weekly basis. Snort can also save all the packets and data associated with the suspicious activity for further analysis (Cox & Gerg 2004; Zhou *et al*., 2010).

For the purpose of data control, a separate physical computer running the Honeywall control system was positioned at the gateway to provide an additional layer of data capture in addition to the data control capabilities. The emulated computers were configured in such a way that, apart from the Linux and Windows servers, some of the simulated computers on the network will go offline automatically during night hours and public holidays to mimic the laboratory environment as closely as possible. Figure 7 illustrates the Honeywall control panel.

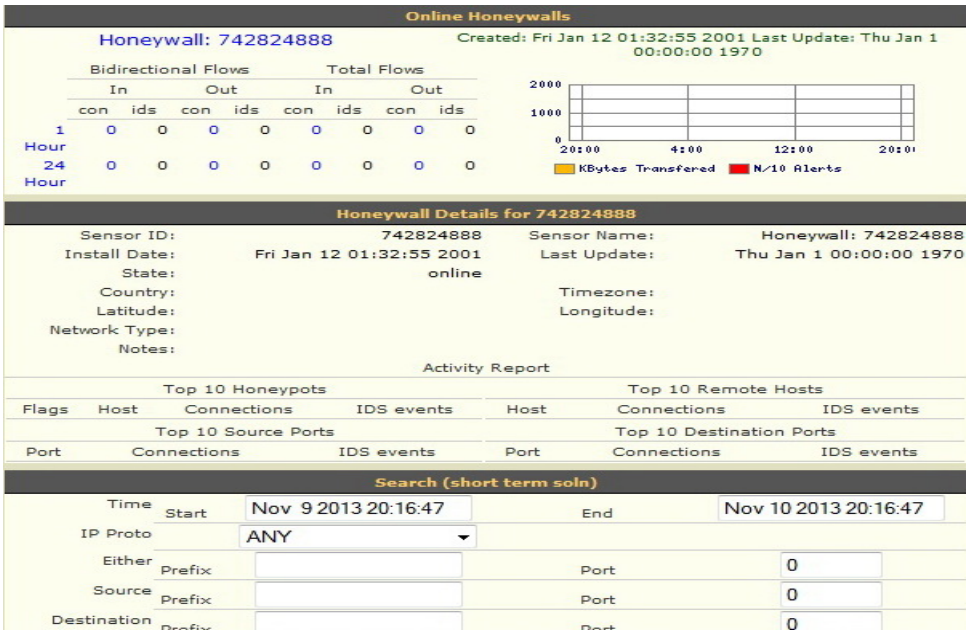


Figure 7: The Honeywall control panel.

5. CONCLUSION

Honeynets represent a new approach in network security. While they should not be considered as replacements for firewalls and IDS systems, they provide a valuable insight to the working and tools used by the hacker community along with the possibility of tracking the intruder's actions step by step. In this paper, a Honeynet is implemented utilising the latest container based virtualisation method, LXC. Compared to other popular virtualisation methods, LXC proved to be the most stable as it provided a good balance of speed and stability.

The properties of LXC based virtualisation allow up to 50 virtual machines running at the same time, thus giving the opportunity to expand and shrink the designed Honeynet dynamically. Currently, a dynamic Honeynet system is being developed to adjust the number of honeypots and emulated services dynamically according to the network traffic and suspicious activity. Up to 7,000 computers and systems can be emulated dynamically at any given time, decreasing the chances of real systems being compromised dramatically. This dynamically scalable Honeynet will provide the highest level of security while keeping the power consumption and usage of hardware resources at a minimum.

REFERENCES

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

Avila, A.E. (2005). *Analyzing Intrusions of a Hybrid Virtual Honeynet*. M.S. Dissertation, The University of Texas at El Paso, El Paso, Texas.

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

Chang, J. C., & Tsai, Y. L. (2010). Design of virtual honeynet collaboration system in existing security research networks. *2010 IEEE Int. Symp. Comm. Inform. Tech (ISCIT 2010)*, pp. 798-803.

Cox, K.J. & Gerg, C. (2004). *Managing Security With Snort and IDS Tools*. O'Reilly Media, Inc, Sebastopol, California.

Honeywall (2014). *The Honeynet Project*. Available online at: http://projects.honeynet.org/honeywall (Last access date: 16 June 2014).

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

Kaur, J., Singh, G. & Singh, M. (2012). Design & implementation of Linux based network forensic system using Honeynet. *Int. J. Adv. Res. Comp. Eng. Tech.*, **1**: 504-508

Konovalov, A. M., Kotenko, I. V., & Shorov, A. V. (2013). Simulation-based study of botnets and defense mechanisms against them. *J. Comp. Syst. Sci. Int.*, **52**: 43-65.

Kuwatly, I., Sraj, M., Al Masri, Z. & Artail, H. (2004). A dynamic honeypot design for intrusion detection. 204 IEEE / ACS Int. Conf. Pervasive Serv. (ICPS 2004), pp. 95-104.

KVM (2014). *Kernel Based Virtual Machine*. Available online at: http://www.linux-kvm.org/ (Last access date: 16 June 014).

Li, P. (2010). Selecting and using virtualization solutions: our experiences with VMware and VirtualBox. *J. Comput. Sci. in Coll.*, **25**: 11-17.

Ligh, M., Adair, S., Hartstein, B. & Richard, M. (2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Wiley Publishing, Hoboken, New Jersey.

Liu, X., Peng, L. & Li, C. (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 Heidelberg, pp. 93-98.

LXC (2014). *LXC – Linux Containers*. Available online at: http://lxc.sourceforge.net (Last access date: 16 June 2014).

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

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

Nmap (2014). *Nmap.org*. Available online at: http://nmap.org (Last access date: 16 June 2014).

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

Rose, R. (2004). *Survey of System Virtualization Techniques*. Oregon State University, Corvallis, Oregon.

Sharma, N. & Sran, S.S. (2011). Detection of threats in Honeynet using Honeywall. *Int. J. Comp. Sci. Eng.*, **3**: 3332-3336.

Shinde, S. (2012). Containers: A New Approach for Virtualization in Cloud Computing. *Int. J. Res. Rev. Eng. Sci.*, **1**: 27-31.

Snort (2014). *Snort*. Available online at: http://www.snort.org (Last access date: 16 June 2014).

Tang, Y. & Li, J. P. (2010). VON/KVM: A high performance virtual overlay network integrated with KVM. *2010 Int. Conf. Apperceiv. Comput. Int. Anal. (ICACIA 2010)*, pp. 129-132.

VMware (2014). *VMware*. Available online at: http://www.vmware.com/company/news/releases/vmw-workstation-082312 (Last access date: 16 June 2014).

VirtualBox (2014). *VirtualBox*. Available online at: https://www.virtualbox.org (Last access date: 16 June 2014).

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

Watson, D. & Riden, J. (2008). The honeynet project: Data collection tools, infrastructure, archives and analysis. *WOMBAT Worksh. Inform. Secur. Threat. Data Collect. Sharing*, pp. 24-30.

Zhou, Z., Zhongwen, C., Tiecheng, Z. & Xiaohui, G. (2010). The study on network intrusion detection system of Snort. IEEE Int. Conf. Network. Dig. Soc. (ICNDS 2010), vol. 2, pp. 194-196.

WIRELESS SPY DEVICES: A REVIEW OF TECHNOLOGIES AND DETECTION METHODS

Dinesh Sathyamoorthy*, Mohd Jalis Md Jelas & Shalini Shafii

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

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

ABSTRACT

Wireless spy devices (WSDs) are surveillance equipment, such as listening bugs or cameras, hidden in objects or covertly placed in rooms. Surveillance using WSDs is one of the main methods of recording conversations for both intelligence gathering as well as criminal charges. However, WSDs have also been abused for nefarious purposes, such as industrial espionage and blackmail. This paper is aimed at reviewing WSD technologies, in terms of types, energy sources and modes of operations. Methods used for detecting WSDs, focusing on radio frequency (RF) detectors, spectrum analysis and nonlinear junction detectors (NLJDs), are also be discussed.

Keywords: *Wireless spy devices (WSDs); active and passive WSDs; radio frequency (RF) detector; spectrum analysis; nonlinear junction detector (NLJD).*

1. INTRODUCTION

Surveillance is defined as the collective action of official gathering of information on persons for the purpose of preventing crime and terrorism, or prosecuting offenders. It includes human and technological gazing where officials observe the physical movements and activities of persons. These observations can be used for identification or may act to advance an investigation as a component of a larger body of evidence, such as in the case of closed-circuit television (CCTV) data. It also involves the acquisition of personal data, which includes the collection of biographical biometric or transactional data on individuals harvested from personal communications, electronic transactions, identifiers, records or other documents. This involves voice or documentary information that can be used in criminal investigations or prosecutions (Bloss, 2007; Lyon *et al*., 2013; Maurer *et al*., 2014).

The annual value of the retail market for surveillance tools increased from almost zero in 2001 to approximately USD 5 billion a year in 2011. This significant increase of demand is due to the 9/11 terrorist attacks, as well as attacks in Bali, Madrid, London and Mumbai, which have underlined the need for better intelligence-gathering capabilities. Furthermore, new technologies have generated vast quantities of data, posing novel challenges for legal and regulatory frameworks, but also creating unprecedented opportunities for law enforcement and intelligence agencies to use that data (Bloss, 2007; Valentino-Devries *et al*. 2011; Maurer *et al*., 2014).

Wireless spy devices (WSDs) are surveillance equipment, such as listening bugs or cameras, hidden in objects or covertly placed in rooms. Surveillance using WSDs is one of the main methods of recording conversations for intelligence gathering as well as criminal charges. In fact, multi-million dollar investigations and trials are often based almost entirely on conversations of people caught making incriminating statements, recorded via WSDs (Peterson, 2001, 2007; Graham & McGowan, 2011; Lyon *et al*., 2013).

However, WSDs have also been abused for nefarious purposes, such as industrial espionage and blackmail. Furthermore, the design and manufacture of WSDs are no longer limited to specialised markets. WSDs are consumer items that are falling in price, and can be bought via mail order

catalogues and the internet. As the value of protected information increases, the threat potential and available WSD technologies also increases (Peterson, 2001, 2007; Lyon *et al*., 2013; Maurer *et al*., 2014).

This paper is aimed at reviewing WSD technologies, in terms of types, energy sources and modes of operations. Methods used for detecting WSDs, focusing on radio frequency (RF) detectors, spectrum analysis and nonlinear junction detectors (NLJDs), will also be discussed. This review is conducted based on the abundance of literature on the related topics, particularly in the field of counter-surveillance, and the authors' experience as members of the Science & Technology Research Institute for Defence (STRIDE) team that conducts WSD detection.

2. WSD TECHNOLOGIES

WSDs are placed in areas where conversations usually occur, such as meeting rooms, offices and vehicles. They can be hidden in wall sockets, light switches, lamps, paintings, ceilings, walls and air vents. In high-level operations, WSDs have also been placed in park benches and cafes frequented by the targets. WSDs are now available in numerous shapes and forms, with many appearing as common everyday items, including electrical adapters, clothes hooks, cups and fake plants. Another type of WSD is that which is worn on the body by an informant or infiltrator, such as in watches, pens, identifications tags and tie pins (Figure 1) (Peterson, 2001, 2007; Davis, 2004; Graham & McGowan, 2011).

Figure 1: WSDs of various shapes and forms.

WSDs require an energy source to operate. In sophisticated devices, small but powerful batteries are used that can last for months. In cheaper models, battery packs are strapped together and hidden along with the microphone and / or camera, though these are more easily detected, and must sooner or later be replaced with fresh batteries (Figure 2). WSDs can also be wired to household or vehicle energy sources (Figure 3) (Peterson, 2001, 2007; Graham & McGowan, 2011).

Figure 2: WSDs powered by 9 V batteries.

Figure 3: A WSD powered by fluorescent light.

WSDs can be categorised into two classes; active and passive. Active WSDs transmit recorded data (voice and / or video) wirelessly via RF to a receiver, which is usually in the vicinity (i.e., a nearby observation post or vehicle) (Figures 4 and 5). The proximity of the receiver will depend on the effective range of the device. In some cases, police have used planes to receive transmissions when it is not possible to get a ground vehicle close enough to a WSD. Buildings and heavy traffic can disrupt transmissions, depending on the device. At times, police have to use abandoned buildings, rooftops or other areas in order to receive transmissions from a device. On the other hand, passive WSDs do not transmit signals, but rather only record data in an internal memory or external memory card (Figure 6). This would make it harder for the device to be detected by scanners, but the surveillance team would require periodic access to it (Peterson, 2001, 2007; Taylor, 2005; Graham & McGowan, 2011).

Figure 4: Active WSDs and their respective wireless receivers.

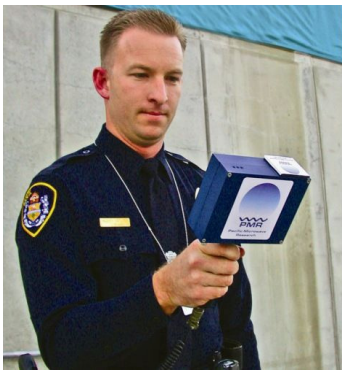


Figure 5: An officer on the ground viewing video received from an active WSD. (Source: Davis (2004))

Figure 6: A passive WSD making use of an external memory card.

Most frequently, small and easily concealed audio microphones (Figure 7) are used for WSDs. Some WSDs also used laser microphones that bounce lasers off a hard surface. Vibrations on the surface caused by sound waves change the way the laser is reflected to the receiver, allowing sound recording (Figure 8) (Peterson, 2001, 2007; Davis, 2004; Graham & McGowan, 2011).

Figure 7: Concealed audio microphones.

Figure 8: A laser microphone, consisting of: Left, an infrared laser transmitter used to detect vibrations on a surface; Right, a phototransistor that picks up the reflected infrared laser light and converts the signal into audio.

Digital cameras continue to offer ever-increasing capability in smaller packages for lower cost. Coupled with the greater ease with which digital imagery can be analysed and manipulated, this has led to the steady decline of analog cameras for most purposes. Microelectronics have allowed these devices to be built very small for easy concealment (Figure 9). There is an inverse relationship between small size and resolution, but this kind of surveillance equipment usually offers adequate capability when used close to the target. Software can be used to collate and evaluate footage, but has

limited ability to identify specific individuals or objects. Cameras which provide imagery outside the visible light spectrum are also available, but are more expensive. Infrared imaging is the most common, but models which provide imaging using other kinds of electromagnetic emissions, such as, x-ray and gamma rays, are also available (Peterson, 2001, 2007; Graham & McGowan, 2011)).

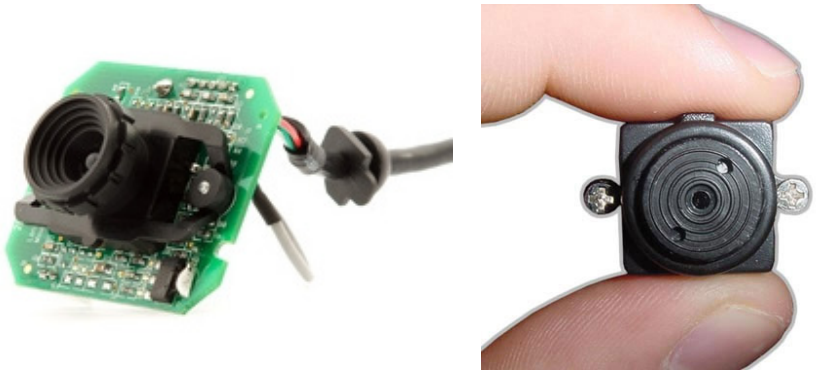


Figure 9: Concealed digital cameras.

3. WSD DETECTION METHODS

3.1 RF Detector

RF detectors (Figure 10) are used to detect RF signals transmitted in given proximities. A RF detector is usually able to sweep a room or area for bugs and warn the user about active RF transmitters (Peterson, 2001, 2007; Taylor, 2005; Savry & Vacherand, 2010; Graham & McGowan, 2011). RF detectors are also used to detect unauthorised wireless communications in restricted areas, which is usually followed by the immediate jamming of the corresponding signal (RABC, 2001; Sambhe *et al.*, 2008; Mishra, 2009; Burke & Owen, 2010). In addition, RF detectors provide important protection to pacemaker users (Pinski & Trohman, 2002a, b; Patel *et al.*, 2007; Seidman *et al.*, 2010), and to those who work in the presence of RF or microwave hazards (Curtis, 2003; MOL, 2009; Wu *et al.*, 2010; TransGrid, 2012).

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

Figure 10: Examples of RF detectors: (a) Lanmda (model LM-DC2) (b) Skynet (model XB-68) (c) Mini Gadgets (model CD-RFLD) (d) Comenzi (model RFS-DT1).

The performance of RF detectors is dependent on two key parameters; operating bandwidth and power level threshold. A number of WSDs are designed to transmit signals with low power levels in order to avoid detection (Peterson, 2001, 2007; Davis, 2004; Taylor, 2005; Graham & McGowan, 2011). A RF detector with low power level threshold is required for detection of such devices. However, if the detector has a power level threshold that is too low, it could cause false alarms, such as from mobile phones or Bluetooth devices. In addition, RF detectors with larger operating bandwidths allow for the detection of a wider range of transmitted signal frequencies (Peterson, 2001,

2007; Taylor, 2005; Savry & Vacherand, 2010). In a previous study (Dinesh *et al.*, 2011), the determination of suitable RF detectors for detection of WSDs was conducted via the measurement of operating bandwidth and power level threshold (Figure 11).

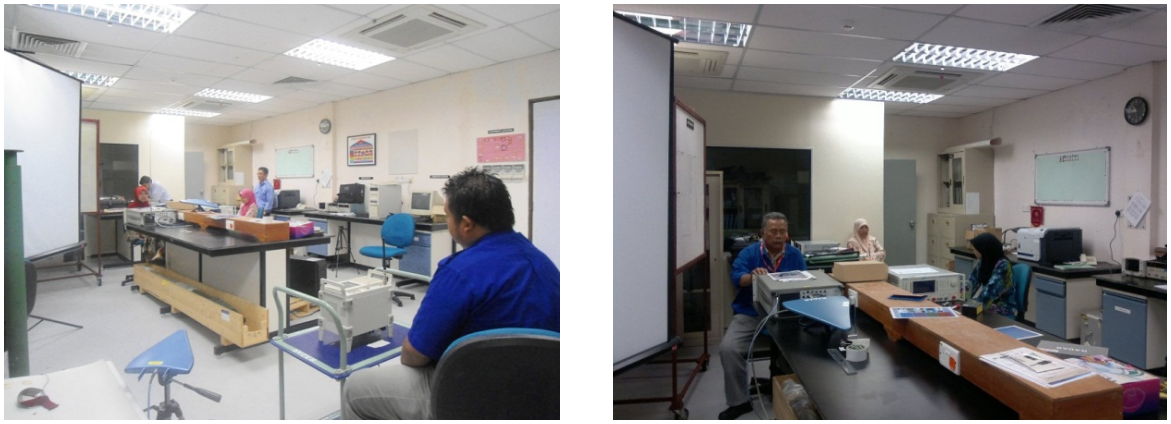


Figure 11: The study conducted in Dinesh *et al.* (2011) on the determination of suitable RF detectors for detection of WSDs via the measurement of operating bandwidth and power level threshold.

While RF detectors are a cheap and effective method for detecting RF transmissions from WSDs, they are not able to provide specific information on the signals detected, such as frequency, power level and content, and hence, can be susceptible to false detections. Furthermore, RF detectors are not high precision meters. The power level thresholds for the RF detectors are not fixed for the respective devices' operating bandwidths, but rather vary with frequency, as demonstrated in Dinesh *et al*. (2011) (Figure 12).

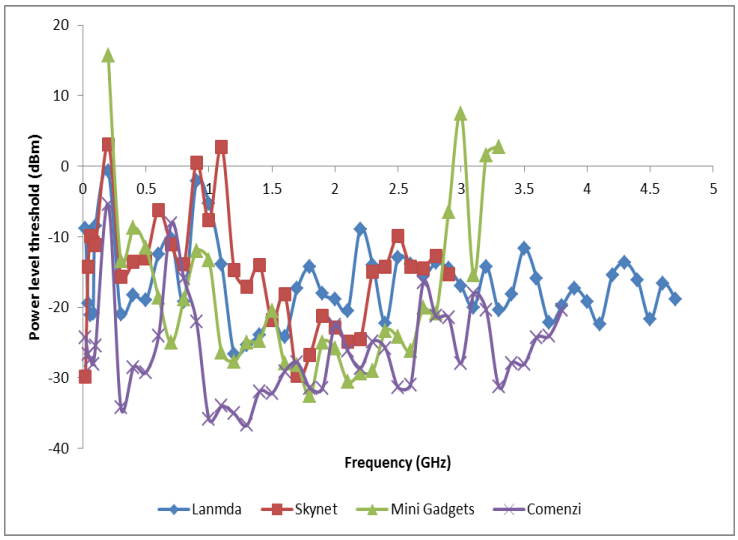


Figure 12: Power level thresholds of the RF detectors shown in Figure 10. (Source: Dinesh *et al.* (2011)

3.2 Spectrum Analysis

A spectrum analyser measures the magnitude of an input signal versus frequency within the full frequency range of the instrument. Its primary use is to analyse RF signals in terms of dominant frequency, power, distortion, harmonics, bandwidth and other spectral components. The display of a spectrum analyser has frequency on the horizontal axis and amplitude on the vertical axis (Witte, 2002; Peterson, 2014). Furthermore, there are spectrum analysers that have been tailor made for the

detection and localisation of anomalous rogue transmissions, such as from WSDs (Figure 13). These spectrum analysers typically have demodulation functions which are used to view the content of the WSD transmissions (Figure 14).

(a) (b) (c)

Figure 13: Recent technologies in signal tracking and detection allow for the fast and effective identification and localisation of RF transmissions from WSDs: (a) Tektronix's H600 RF Hawk (b) Rohde & Schwarz's PR100 (c) REI's Oscor Green.

Figure 14: REI's Oscor Green spectrum analyser being used to demodulate the transmission content of a WSD.

Spectrum analysers are also used in wireless communications to determine out-of-band and spurious emissions. For example, cellular radio systems must be checked for harmonics of the carrier signal that might interfere with other systems operating at the same frequencies as the harmonics. Engineers and technicians are also very concerned about distortion of the message modulated onto a carrier. Spectrum monitoring is another important frequency-domain measurement activity. Government regulatory agencies allocate different frequencies for various radio services, such as broadcast television and radio, mobile phone systems, and police and emergency communications. It is critical that each of these services operates at the assigned frequency and stays within the allocated channel bandwidth. Transmitters and other intentional radiators often must operate at closely spaced adjacent frequencies. A key performance measure for the power amplifiers and other components used in these systems is the amount of signal energy that spills over into adjacent channels and causes interference (Webb, 2007; Molisch, 2011; Peterson, 2014).

3.3 Nonlinear Junction Detector (NLJD)

The methods discussed thus far are only applicable to active WSDs, whereby detection is based on identification of signals transmitted by the WSDs. However, these methods are not applicable for passive WSDs, which do not transmit signals.

NLJDs (Figure 15) are designed for detecting devices that contain semiconductor elements, such as diodes, transistors and circuits. The operating principle of a NLJD is based on transmission of a clean RF signal, with no harmonics or audio modulation, on the investigated object, and analysis of levels of second and third harmonic signals reflected from the object. By comparing the received signal strengths of these two harmonics, the operator can distinguish if the target location contains a dissimilar metal non-linear junction, such as some rusty nails, or an actual semiconductor (PN) junction (Figure 16). The boundary areas of PN junctions are nonlinear, in that when lluminated with a RF carrier, they will generate successive harmonics of the initial illumination carrier signal, without requiring the item to be powered on. In nature, a similar junction is often created between two dissimilar metals of a catalyst. A true PN junction and a natural junction can be differentiated by comparing the received signal strengths of the different harmonics generated. True PN junctions generate strong even harmonics (second, fourth, sixth, etc.) while dissimilar metals create strong odd harmonics (third, fifth, seventh, etc.). In addition, a harmonic signal from a true PN junction will be quiet when audio demodulated. Since the illumination RF carrier is clean and unmodulated, the even-order harmonics will also be clean and unmodulated. In comparison, the odd-order harmonics from dissimilar metals tend to be noisy when audio demodulated (GIG, 2010; GBPPR, 2010; Graham & McGowan, 2011; WCS, 2014).

Figure 15: NLJDs being used to detect WSDs.

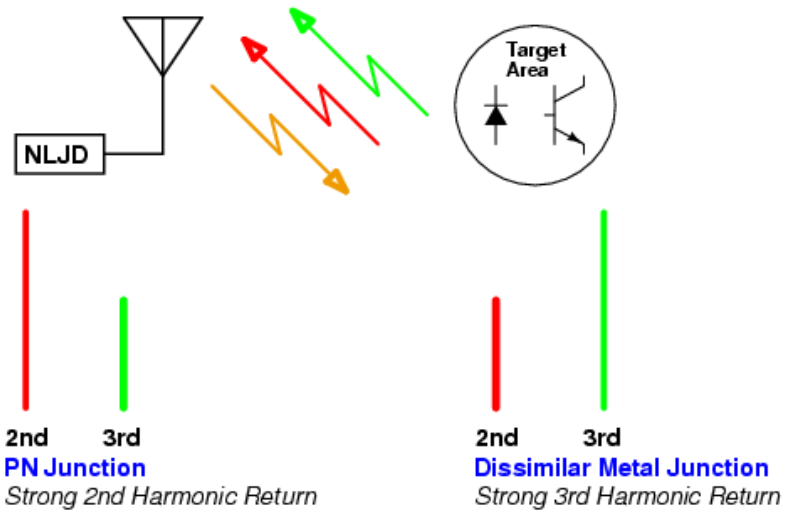


Figure 16: Operation of a NLJD.
(Adapted from GBPPR (2010))

The conversion efficiency of the illuminated NLJD signal to harmonic signals is determined by the harmonic cross section of the nonlinear components in the WSD. The greater the cross section, the larger the amplitude of the radiated harmonic energy. The diode elements in a WSD have a harmonic power output curve that is exponential. However, there is a saturation limit that is reached after a certain level of irradiation. When a nonlinear junction reaches saturation, no further increase in harmonic amplitude occurs even if irradiation power is increased. The amplitude of the harmonic signal produced by a nonlinear junction is very strongly dependent on transferring power from the air to the nonlinear junction. This is influenced by the resonant frequency of the junction which is derived, in part, from the area and thickness of the junction. This resonance is directly related to frequency of illumination and hence, it is imperative for maximum detection probability (maximum excitation of the nonlinear junction) that the frequency of the NLJD be dynamic or tunable, given the wide impedance variations expected to be found in WSDs (WCS, 2014).

A NLJD typically has an antenna and a control unit. The antenna is mounted on an extendable pole, and is used to emit and collect the signals (with a duplexer). The control unit is usually a multiple channel, highly sensitive radio receiver tuned to specific second and third harmonic frequencies. The detector automatically determines the best receiving frequency channel free of noise and distortion in order to provide maximum sensitivity for the detection (GIG, 2010; GBPPR, 2010; Graham & McGowan, 2011; WCS, 2014).

4. CONCLUSION

This manuscript provided a review of WSD technologies and methods for detection of WSDs. WSDs are available in numerous shapes and forms, with many appearing as common everyday items, using internal batteries, or external household or vehicle energy sources. WSDs can be categorised into two classes: active, which transmits recorded data via RF; and passive, which only records the data. While RF detectors and spectrum analysis are effective methods for detection of active WSDs, NLJDs are more appropriate for detection of both active and passive WSDs.

ACKNOWLEDGEMENT

The figures in this manuscript were obtained from casual browsing of the internet. The formation of STRIDE's WSD detection team in June 2012 was the brainchild of Datuk Dr. Abdul Ghaffar Ramli, former Director-General of STRIDE, and the authors are grateful to him for his guidance and support.

REFERENCES

Bloss, W. (2007). Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects. *Surveill. Soc.*, **4**: 208-228.

Burke, T.W. & Owen, S.S. (2010). Cell phones as prison contrabands. *FBI Enforcement Bull.*, **12**: 10-15.

Curtis, R. (2003). *Introduction to Radio Frequency Radiation*. Occupational Safety & Health Administration (OSHA), US Department of Labor, Washington D.C.

Davis, B. (2004). Spy gear: Modern surveillance tools use the newest technology to catch crooks on the sly. *Police Law Enforcement Mag.*, **28**: 38-43.

Dinesh, S., Nur Atiqah, J., Mohd. Faudzi, M., Mohd Idris, I., Shalini, S., Aliah, I., Zainal Fitry, M.A., Siti Zainun, A. & Mohd Hasrol Hisam, M.Y. (2011). Determination of suitable RF detectors for detection of wireless spy devices. *Defence S&T Tech. Bull.*, **4**: 183-196.

GBPPR (Green Bay Professional Packet Radio) (2010). *GBPPR Non-Linear Junction Detector*. Available online at: http://gbppr.dyndns.org/mil/non/index.html (Last access date: 19 May 2014).

GIG (Granite Island Group) (2010). *Nonlinear Junction Detector Review and Tutorial*. Granite Island Group (GIG), Boston, Massachusetts.

Graham, B. & McGowan, K. (2011). *101 Spy Gadgets for the Evil Genius, 2nd Ed*. McGraw-Hill, New York.

Lyon, D. (2013) Surveillance technologies and social transformation: Emerging challenges of socio-technical change. In Lee, L.F., Leung, L., Qiu, J.L. & Chu, D.S.C. (2013), *Frontiers in New Media Research*. Routledge, New York.

Maurer, T., Omanovic, E. & Wagner, B. (2014). *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*. New America Foundation, New York.

Ministry of Labour (MOL) (2009). *Radiofrequency and Microwave Radiation in the Workplace*. Ministry of Labour (MOL), Ontario.

Mishra, N.K. (2009). Development of GSM - 900 mobile jammer: An approach to overcome existing limitation of jammer. *Fifth IEEE Conference on Wireless Communication and Sensor Networks (WCSN)*, 15th-18th December 2009, Allahabad, India.

Molisch, F.A. (2011). *Wireless Communications*. John Wiley & Sons Ltd., Chichester, West Sussex.

Patel, M.B., Thaker, J.P., Punnam, S. & Jongnarangsin, K. (2007). Pacemaker interference with an iPod. *Human Rhythm*, **4**: 781-784.

Peterson, B. (2014). *Spectrum Analyser Basics*. Agilent Technologies Inc., Santa Clara, California.

Peterson, J.K. (2001). *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications*. CRC Press, Boca Raton, Florida.

Peterson, J.K. (2007). *Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications.* Auerbach Publications, Boca Raton, Florida.

Pinski, S.L. & Trohman, R.G. (2002a). Interference in implanted cardiac devices, Part I. *Pace*, **25**: 1367-1381.

Pinski, S.L. & Trohman, R.G. (2002b). Interference in implanted cardiac devices, Part II. *Pace*, **25**: 1496-1509.

Radio Advisory Board of Canada (RBAC) (2001). *Use of Jammer and Disabler Devices for Blocking PCS, Cellular & Related Services*. Radio Advisory Board of Canada (RBAC), Ottawa, Ontario

Savry, O. & Vacherand, F. (2010). Security and privacy protection of contactless devices. In Giusto, D., Iera, Morabito, G. & Atzori (Eds.), *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*. Springer, New York, pp. 409-420.

Seidman, S., Randall, Brockman, R., Lewis, B.M., Guag, J., Shein, M.J., Clement, W.J., Kippola, J., Digby, D., Barber, C. & Huntwork, D. (2010). In vitro tests reveal sample radiofrequency identification to implantable pacemakers and implantable cardioverter-defibrillators. *Human Rhythm*, **7**: 99-107

Sambhe, V.K., Kale, D.S.K., Wasule, A. & Neema, S. (2008). Antenna for mobile phone jammer . *First International Conference on Emerging Trends in Engineering and Technology*. 16-18 July 2008, G. H. Raisoni College of Engineering, Nagpur, India.

Taylor, C. (2005). *The Red Balloon*. Pinpoint Productions Inc., Vancouver, Canada.

TransGrid (2012). *Safe Work Practices on Radio Frequency Transmitting Apparatus*. TransGrid, Sydney.

Valentino-Devries, J., Angwin, J. & Stecklow, S. (2011). Document trove exposes surveillance methods. *Wall Street J.*, 19 November 2011.

Wu, C.Y., Lee, T.S. & Hsue, C.W. (2010). Mobile phone users and base stations versus human health concern. *2010 Asia Pacific Symposium on Electromagnetic Compatibility (APEMC)*, 12-16 April 2010, Beijing, China.

WCS (Waypoint Counter Surveillance) (2014). *About Non Linear Junction Detectors*. Available online at: http://www.waypointcs.ca/tscm-equipment-sales/about-non-linear-junction-detectors.php (Last access date: 19 May 2014).

Webb, W. (2007). *Wireless Communications: The Future*. John Wiley & Sons Ltd., Chichester, West Sussex.

Witte, R.A. (2002). *Electronic Test Instruments: Analog and Digital Measurements*. Prentice Hall, New Jersey.

ONLINE INFORMATION SEARCH BEHAVIOUR AMONG RESEARCHERS IN STRIDE

Rozita Md Salleh

Research and Strategic Studies Branch, Human Resources & Technical Support Division (BPSM&KS), Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

Email: rozita.salleh@stride.gov.my

ABSTRACT

The purpose of this paper is to identify the standard practices of researchers in Science and Technology Research Institute for Defence (STRIDE) in finding relevant online information to support their research. The study was conducted using the qualitative research approach to study the search behaviour used to retrieve relevant online information for their research projects and publications specifically in defence areas. Several interviews were conducted and the common practices carried out by researchers were identified. It was found that the researchers have their own preferences in conducting online searches. The study focused on four main themes as guidelines in collecting the data, which are search options, use of keywords, level of information relevancy and satisfaction. The findings indicated that most of the researchers use common search engines, in particular Google. Others prefer using websites with specific fields that meet their research requirements. Keyword search, using either single or multiple terms, is the most common technique used. Most of the searches conducted gave about 70% information relevancy. Despite the high relevancy of documents retrieved, the online search practices result in only 40% researchers' satisfaction.

Keywords: *Online information search behaviour; search engines; keywords; information relevancy; user satisfaction.*

1. INTRODUCTION

The use of internet has increased significantly as it connects people globally and provides huge amounts of information. According to Levene (2010), Google has become the most popular search engine among different levels of searchers and navigators. With its capability in providing quick retrieval of information, it was estimated that the growth rate was 200 million of web pages per day as at 2010. In terms of queries, Google received more than over 40,000 queries per second. The challenges highlighted in navigating using search engines are a result of the current size of websites, the amount of duplications, dynamic nature and website quality. Despite these challenges, accessing information online has become one of the main activities for researchers in getting current and reliable information to support their studies. For example, according to Sanjay & Praveen (2013), arts and science research scholars from Banaras Hindu University had the highest number of hours per week spent on online resources that is from six to ten hours for 19 (31.14%) arts respondents from the total number of 61, and 22 (28.20%) science respondents from the total number of 78. These two groups had different resource preferences with the art respondents preferring e-books and electronic theses, and the science respondents preferring e-journals.

Researchers have realised that online information can be retrieved within seconds, providing great options for their research and additional supporting data. Even though a lot of information can be acquired from other printed resources, these types of information require more time and patience to be

accessed and used. Since a huge amount of information is available on the internet, and quick retrieval functions are provided by search engines and databases, these have resulted in full reliance on electronic collections. Morris *et al.* (2010) found that searching using search engines is more useful as compared to other social media based on the shorter response time it consumes. Besides that, integrating the use of search engines and social media could improve the information seeking experience as these increase the users' satisfaction. Searchers can request for help from other people, by using Facebook or Twitter, to gather information. Although some requests do not gather information immediately, it does provide more customised answers to the questions and suggestions to search for more relevant materials.

Dempsey & Russel (1997) noted that the term 'information resources' is often used to refer to books, images, bibliographic records, websites and other types of resources that exist in the collection of databases. Databases are the most common information resource accessed by researchers. A huge collection of research articles have been published, in addition to other types of information in various formats being available. Databases allow access to their collections by providing various search options. They also provide features that allow researchers to choose their options in terms of subject category, such as engineering, medical, chemistry, physics or pure science. Researchers will need to further identify their information needs by providing the document titles, and specifying the type of format of the documents needed and several other options to narrow down their search. In addition, inverted file processes have enabled databases to match researchers' queries with the document collection within several seconds. According to Zobel & Moffat (2006), there are two components of index structure - search structure or vocabulary stores, and sets of inverted list - that make inverted files the most efficient index structure for text query evaluation.

On the other hand, some researchers prefer using normal search engines, such as Google and Yahoo, to access the information that they need. Although it results in more time consumed to get to the right information, they anticipate that search engines give high quality and quantity of information retrieved. Padma *et al*. (2013) described information seeking behaviour as various actions performed including expression of information needs, seeking the information, evaluation and selection, and the satisfaction level achieved in using the selected information. Their study on a group of postgraduate students from the School of Economics at Madurai Kamaraj University indicated that Google is frequently used, by 40% of the total respondents, followed by Yahoo and Alta Vista (22%). The remaining respondents preferred using other search engines.

Modern retrieval systems, including search engines, have provided search tips to facilitate retrieval of relevant information. However, problems arise when the search terms used are too broad or carry less meaning. This result in low quality and high quantity of irrelevant documents being retrieved (Osinski & Weiss, 2005). Furthermore, although search tips are available and require very little effort to understand their applications, the level of usage and reference to those basic search tips are questionable. Sutcliffe *et al*. (2000) found that novice researchers have poor search performance as compared to experts who use more query iterations, including broadening and narrowing strategies. Novice researchers normally conduct their online information searches using trial and error until the information needed is retrieved.

According to Manikandan *et al*. (2013), from the total of 710 respondents from five selected universities in India, 12.28% of researchers prefer print copy and 29.83% researchers prefer electronic copy of materials. The study shows that a bigger percentage of researchers appreciate the advantages of using the electronic resources and the convenience it provides. The information they gathered has enabled all the researchers to use new sources for their research as compared to their previous information searches. The formal training programme to search for scientific or technical information has improved their skills in retrieving the relevant information and facilitates their searchers.

This study is aimed at identifying researchers' knowledge and awareness on the facilities provided to assist in any online information search conducted. The study is focused on online information search behaviour among researchers in the Science and Technology Research Institute for Defence

(STRIDE). The searches conducted by the researchers pertain to their work in various fields of defence science & technology, including electronics, communications, surveillance and geospatial technologies; personal protection equipment (PPE), and food and rations; chemical, biological, radiological and nuclear (CBRN) defence; aeronautics and vehicular technologies; weapons, propulsion and ballistics; and maritime and ship technologies. The objectives of this study are to determine:

1) How the researchers access online information
2) Whether the retrieved documents contain relevant information for the researchers
3) How the researchers rate their satisfaction of the online information searches.

2. METHODOLOGY

Several interview sessions were conducted to gather data on the search behaviours of the researchers for research and publication purposes. The interview questions were based on the research objectives. Since the telephone conversation is known to incur less costs and requires shorter time to complete, this technique was used. Furthermore, the selected respondents have experience in conducting and leading research and development activities. Five researchers were identified to provide the most appropriate data related to this study. These respondents had roles as research project leaders and conduct frequent online searches. From the interviews, it was found that these researchers have never attended special courses related to online search techniques but were aware of the search aids available in the search engines. The purpose of selecting respondents from various backgrounds was to gather more reliable and accurate data.

The respondents were approached by introducing the objectives of the study and explaining the focus of the evaluation. The questions that were asked include how they conduct searches, the use of keywords, the relevancy of retrieved documents, and researchers' satisfaction on the search conducted. During the data collection process, the respondents were encouraged to provide more details on their search experiences.

3. RESULTS & DISCUSSION

Based on the interview data collected, the online information search behaviour of the researchers was examined based on the following four themes:

3.1 Search Options

The researchers identify their needs in the general topic before selecting the appropriate website or search engine. The data showed that most of the researchers choose to conduct their searches using Google, while some prefer to use specific websites that they have identified as containing the related research topics. This option is taken based on their experience and knowledge in conducting online information searches. Based on frequent searching through the websites, researchers find specific websites that contain relevant materials that are tailored to their needs. Due to the unavailability of subscribed databases by the agency, some researchers try to get access to databases in the Malaysian Ministry of Defence and universities.

3.2 Use of Keywords

The author expected that the researchers would attempt to insert whole sentences into their search fields, but the percentage for this was very low. Through experience, the researchers are able to select and use the right single or multi-keywords for their searches and retrieve the information needed.

Most of them agreed that search engines are able to provide related information even when utilising single keywords. Formulating the search terms is common to all information searchers as they believe the search terms inserted will return a list of hits they required. This corresponds to the findings of Palma *et al*. (2013) that the use of keyword search is the highest among postgraduate students. Author search (28%) has become the second mechanism to search for online materials followed by title search (22%), while very few respondents use subject search (10%) to fulfil their requirements.

Kumar (2012) further examined the trend of searchers' attitude, particularly in using Google and OPAC in the context of Indian university settings. In comparison to the author's findings, very few searchers change their strategies when unsuccessful searches were attained. Only 1.4% of research scholars, and 10% of faculty members and postgraduate students change keywords or check for typological errors. In terms of academic majors, many turns to librarians to seek for required materials.

3.3 Information Relevancy

Once the list of documents is retrieved, the researchers will go through the list and identify whether the content is relevant to their needs. Once they have assessed the selected documents, they will conduct further searches by inserting synonyms to further explore the potential results. Most of the researchers agreed that they get more than 70% relevancy from the retrieved documents.

Ozmutlu (2005) found that keyword format queries using Google showed statistically significant differences in the mean relevancy scores as compared to Askjeeves. The study further proved that the selection of search engine affects the relevancy scores. Therefore, pre-assessing and identifying the most relevant search engines or databases is important for researchers before information searching is conducted.

3.4 Researchers' Satisfaction

Based on the data collected, it was found that only 40% of the researchers are satisfied with the results retrieved using search engines. The lack of satisfaction with the results retrieved causes new keywords to be generated and used. The formulation of new keywords helps the researchers to obtain better content. Through the first few searches, researchers managed to capture more appropriate words that contribute to their fact finding. They even learned and explored more useful websites that focus on their subject search. Besides getting more hits in multiple searches, limited content of the subject required has also resulted in dissatisfaction. Some of the search processes halt with the retrieval of low quality or older research materials.

The lack of satisfaction is also caused by websites that do not allow free reading or downloading of materials. Paid materials are normally more relevant to the researchers' needs but require users to log in, and purchase them or be a member to enable access to unlimited material. This has become a barrier that causes disappointment among the researchers. Mastering vocabulary gives more chance for users in gaining access to required materials. To this end, the availability of vocabulary lookup tables help in the searching process for different words but with the same meaning. Most researchers realise this function but the usage is minimal as they do not apply the nesting technique that helps broaden or narrow the search.

4. CONCLUSION

Based on the findings discussed above, researchers have better options in getting access to the right materials through the number of searches they conduct and the specific websites that they come across based on their past online searchers. Through this, they gain more advantages in retrieving their

needed materials in shorter time, with more relevant materials displayed by the search engines. The use of keywords has become the major technique to access the information as compared to other mechanisms such as subject, title and author searches. Most of the keyword search techniques result in successful searches. Despite the ability of Google to enable the researchers to grab the most relevant documents and produce very large number of hits, the researchers' satisfaction towards the content of the documents is moderate.

The study did not include other techniques of data collection, such as observation. Therefore, the actual output or documents retrieved is not known in detail, which could have affected the results. There was also no involvement of junior research officers in the interviews, who are generally more exposed to better search techniques that should give better results for the findings. Furthermore, this study focused on a limited environment where most of the researchers have access only to search engines, but not online databases. It is recommended that future researches should cover a wider scope in order to study search behaviours among researchers using online databases.

REFERENCES

Dempsey, L. & Russell, R. (1997). Clumps or organized access to printed scholarly publications: outcomes from the 3rd model workshop. *Program*, **31**: 239-50.

Kumar, S. (2012). The impact of demographic of user on patterns of usage on search engines and OPAC. *Libr. Rev.,* **61**: 172-187.

Levene, M. (2010). *An Introduction to Search Engines and Web Navigation*. John Wiley and Sons, New Jersey.

Manikandan, G., Mohamed Ismael, S. & Nagarajan, M. (2013). Impact of Information Technology on Information Seeking Behavior of the Users: An Empirical Study. *J Adv. Libr. Inform. Sci.*, **1**: 60-64.

Morris, M.R., Teevan, J., & Panovich, K. (2010). A comparison of information seeking using search engines and social networks. *4th Int. AAAI Conf. Weblogs Soc. Media*, 23-26 May 2010, George Washington University, Washington D.C.

Osinski, S. & Weiss, D. (2005). A concept-driven algorithm for clustering search results. *IEEE Intell. Syst.*, **20**: 48-54.

Ozmutlu, S. (2005). Performance of question-based vs. keyword-based search engines and effect of web user characteristics on search engine performance. *Online Inform. Rev.*, **29**: 656-675.

Padma, P., Ramasamy, K & Sakthi, R. (2013). Information needs and information seeking behaviour of post graduate students of School of Economics at Madurai Kamaraj University: A user survey. *Inter. J. Educat. Res. Technol.*, **4**: 33-42.

Sanjay, K. & Praveen, S. (2010). Information seeking pattern in electronic, environment of sciences and arts researchers: a comparative study. *Braz. J. Inform. Sci.*, **7**: 57-66.

Sutcliffe, A., Ennis, M. & Watkinson, S.J. (2000). Empirical studies of end-user information searching, *J. Am. Soc. Inform. Sci.*, **51**:1211-31.

Zobel, J. & Moffat, A. (2006). Inverted files for text search engines. *ACM Comput. Surv.*, **38**: 6.1-6.56.