Two-Call Index Based Internet Traffic Sharing Analysis in Case of Cyber Crime Environment of Computer Network

Dr. Sharad Gangele[1], Prof. (Dr.) Ashish Dongre[2]
[1]Associate Professor, Department of Computer Science, R.K.D.F., University, Bhopal (M.P.), India
[2]Vice-Chancellor, R.K.D.F., University, Bhopal (M.P.), India
[1]sharadgangele@gmail.com
[2] ashish.dongre@gmail.com

Abstract-**While there are many benefits from the Internet, it has also become a powerful tool in the hands of those wishing to engage in criminal activities. Cyber crime encompasses any criminal act dealing with computers and networks, due to huge internet traffic load every service provider want to capture much more traffic share in their account as compare to competitive service provider. A model based internet traffic share problem was initiated by Naldi (2002). The basic idea of Naldi (2002) was extended by Shukla, Thakur and Tiwari(2010) in which limitation of call-by-call converted in to two-call with the addition of one more cyber crime state. In this paper we consider same approach for different kind of users with index formation. This paper presents an index based internet traffic share analysis for the better judgement of users behaviour in case when two operators are in competitive mode. Simulation study is performed to support the mathematical findings.**

Keywords-**Index (I), Internet Traffic (IT), Markov Chain Model (MCM), Two-Call (TC).**

I. INTRODUCTION

In the present scenario of research internet crime is major challenge for law enforcement agencies. Internet criminals not only can hide their identities but can use numerous internet pathways to make tracking their activities very difficult. Cyber crimes appear when any illegal activities are committed through the use of a computer and the internet. In this paper we categories two type of user (a) Crime user (CU) (b) Non Crime user (NCU).CU means a user who perform cyber crime after susses call connection whereas NCU indicate that users who never opt to cyber crime on internet after a successful call connectivity.CU perform the activity like existing federal laws for identity theft, telemarketing and Internet fraud, credit card theft, securities fraud, and gambling etc. Naldi (2002) developed a mathematical model for the problem of internet traffic sharing between two competitive operators. This model was extended by Shukla, Thakur and Tiwari(2010) with increment of two call based cyber crime state and calculate some new traffic share expressions. This paper presents two-call index based internet traffic share analysis for better judgement of behaviour of cyber criminals on the contribution of Shukla, Thakur and Tiwari (2010).

II. A REVIEW

In the recent trend, application of markov chain is utilized by many software developers and researchers for the purpose of transition behaviour of any system. Stochastic modelling for space division switching was proposed by Shukla, Gadewar, and Pathak (2007) in a new look in the area of networking. Dorea, Cruz and Rojas (2004) discussed an approximate result in case of non homogeneous markov chain and develop some application for it. Naldi (2002) derived internet traffic share expression for two operator environment and further extend it in multi operator case. Francini and Chiussi (2002) examine the quality of services for unicast and multicast flow stage in packet switching behaviour and develop a methodology for it. Medhi (1991) has given a fundamental aspect of markov chain model and discussed various applications related to randomness. Shukla and Thakur (2007) focused on internet traffic sharing analysis for the judgement of behaviour of cyber criminals in multi operator environment. Agarwal and Kaur (2008) attempted for reliability analysis of fault-tolerant multistage interconnection networks and develop some new concept. Shukla, Jain and Ojha(2010) examined deadlock index analysis of multi-level queue scheduling in operating system using markov chain. Tiwari, Thakur and Shukla (2010) advocate crime based user behavior analysis and derived the expression of traffic share for different categories user. Naldi (1999) initiated measurement based modelling approach for internet dial-up access connections and has given a view point approach by using markov chain model.Shukla, and Thakur(2009) have given a mathematical approach for rest state analysis between two operator environment to find out traffic share status which are in competitive mode. Shukla *et al.*(2009) analyzed rest state based internet traffic share analysis between two operator environment. Shukla *et al.*(2009) explored the knowledge of share loss of traffic share in multi market situation and find various expression for it. Shukla and Gadewar(2007) attempted for cell movement in a knockout switching through stochastic modeling and develop a new framework of transition behavior of a system where as Shukla *et al.*(2007) conducted a study for Space-Division Switches with the help of same kind of modeling. One more contribution is obtained by Shukla *et al.*(2010) and find the effect of disconnectivity factor of internet traffic sharing in two competitive operator environment. Shukla and Thakur(2010) have put on a new look on index based internet traffic share problem for different categories of users. Thakur and Shukla(2010) have innovatively presented Iso-share analysis of internet traffic sharing in presence of favoured dis-connectivity and find disconnectivity is in favour of an operators. Shukla and Singhai(2011) proposed a novel approach for browser sharing analysis when two browser installed in a computer system by using markov chain where as Shukla *et al.*(2011) have reviewed the elasticity analysis of same kind of modelling and derive some new results. Shukla *et al.*(2011a,b) have given a thought on elasticity analysis for different kind of modeling and find rate of change with respect to blocking parameter. Shukla *et al.*(2012a,b,c,d) explored a markov chain model based study and present least square based curve fitting application of internet traffic sharing with the support of confidence interval. Gangele *et al.*(2014a,b,c) focused on area estimation of internet traffic sharing problem with the support of trapezoidal rule usually applies in numerical quadrature.

III. ASSUMPTIONS FOR SYSTEM AND USER BEHAVIOUR [AS DEFINED SHUKLA, TIWARI AND THAKUR (2010)]

a. The user chooses, operator O_1 with probability p or operator O_2 with probability (1 - p).
b. When first attempt of connectivity fails he attempts one more to the same operator, and thereafter, switches to the next where two more consecutive attempts may appear. This we say "two-call-basis" attempts for call connectivity.
c. User has two choices after each failed attempt;
   a. he can either abandon with probability p_A or
   b. switch to the other operator for a new attempt.
d. The blocking probability that a call attempt fails through the operator O_1 is L_1 and through O_2 is L_2.
e. If the call for O_1 is blocked at k^{th} attempt (k > 0) then in $(k + 2)^{th}$ user shifts to O_2.
f. Whenever call connects through either of O_1 or O_2 we say system reaches to the state of success after n attempts.
g. User can terminate the connectivity attempt process which is marked as abandon state A with probability p_A (either O_1 or from O_2).
h. A successful call connection has a marketing package related to cyber-crime, denoted as C, with attraction probability $(1 - c_1)$ and detention probability $(1 - c_2)$.
i. After connectivity, user has two choices either to do or cyber-crime or to do usual web surfing through Internet (with probability c_1). This choice is treated as an attempt related to web connectivity.
j. Attempt means call-connecting attempt or surfing attempt.
k. User may come-back to usual surfing whenever willing (with probability c_2) or may continue with cyber crime depending on attraction of marketing plan.
l. From crime, user can neither abandon nor disconnect.
m. From state of normal surfing, user can not abandon.
n. State non-crime and abandon are absorbing state.

IV. MARKOV CHAIN MODEL [See Shukla, Tiwari And Thakur (2010)]

Using above hypotheses about user's behavior it can be modeled by a five-state discrete-time Markov chain $\{X^{(n)}, n \geq 0\}$ such that $X^{(n)}$ stands for the state of random variable X at n^{th} attempt (call or surfing) made by a user over the state space $\{O_1, O_2, NC, A, C\}$ where,

State O_1: User attempting to connect a call through the first operator O_1.

State O_2: Corresponding to a call through second operator O_2.

State NC: Success (in connectivity) but no cyber-crime.

State A: User leaving (abandon) the attempt process.

State C: Connectivity gained and cyber-crime.

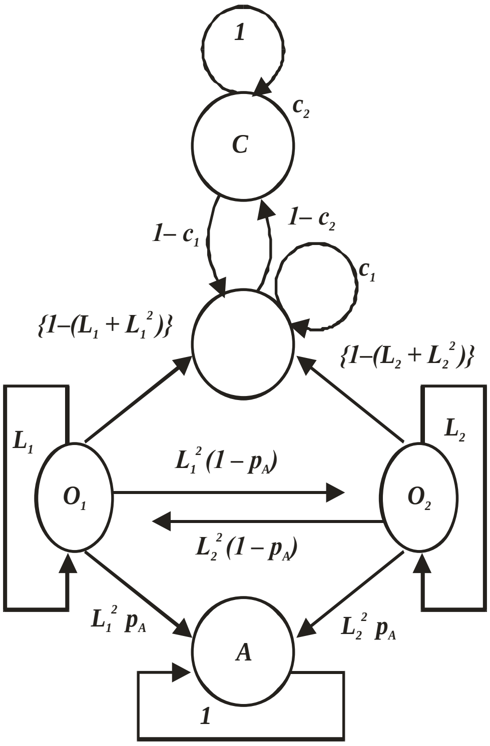

Fig 4.1:- Transition Diagram of Model [As per Shukla, Tiwari and Thakur (2010)]

The connectivity attempts between two operators are on two-call basis, which means if the call for O_1 is blocked in $k^{(th)}$ attempt ($k > 0$), then in $(k + 2)^{th}$ user shifts to O_2. When call connects either through O_1 or O_2 the system reaches to the state of success (NC) and does not perform cyber crime in next attempt with probability c_1. From state C, user cannot move to states O_1, O_2 or A without passing through NC. The A is absorbing state.

V. TRANSITION MECHANISM IN MODEL AND PROBABILITIES [As Suggested By Shukla, Tiwari And Thakur (2010)]

Rule 1: User attempts to O_1 with initial probability p (based on QoS the O_1 provides).

Rule 2: If fails, then reattempts to O_1.

Rule 3: User may succeed to O_1 in either of one attempt or next. Since the blocking probability for O_1 in one attempt is L_1, therefore, blocking probability for O_1 in the next attempt is:

= P [O_1 blocked in an attempt]. P [O_1 blocked in next attempt / previous attempt to O_1 was blocked] = $(L_1.L_1) = L_1^2$

The total blocking probability is $(L_1 + L_1^2)$ inclusive of both attempts. The success probability for O_1 is $[1-(L_1 + L_1^2)]$ Similar for $O_2 = [1-(L_2 + L_2^2)]$

Rule 4: User shifts to O_2 if blocks in both attempts to O_1 and does not abandon. The transition probability is:

= P [O_1 blocked in an attempt]. P [O_1 blocked in next attempt/previous attempt to O_1 was blocked]. P [does not abandon attempting process] = L_1^2 (1- p_A) Similar for $O_2 = L_2^2$ (1- p_A).

Rule 5: User either abandons the system atleast after two attempts to an operator, which is a compulsive with this model. This leads to probability that user abandons process after two attempts over O_1 is:

= P [O_1 blocked in an attempt]. P [O_1 blocked in next attempt/previous attempt to O_1 was blocked]. P[abandon the attempting process] = $L_1^2\, p_A$ Similar happens for $O_2 = L_2^2\, p_A$

Rule 6: for, $0 \leq c_1 \leq 1$ and $0 \leq c_2 \leq 1$ we have

$$P\left[X^{(n)} = C \big/ X^{(n-1)} = NC\right] = 1 - c_1 \quad \text{...(5.1)}$$

$$P\left[X^{(n)} = NC \big/ X^{(n-1)} = NC\right] = c_1 \quad \text{...(5.2)}$$

$$P\left[X^{(n)} = NC \big/ X^{(n-1)} = C\right] = c_2 \quad \text{...(5.3)}$$

$$P\left[X^{(n)} = C \big/ X^{(n-1)} = C\right] = 1 - c_2 \quad \text{...(5.4)}$$

VI. TRANSITION PROBABILITY BETWEEN STATES [See Shukla, Tiwari and Thakur (2010)]

Define a Markov chain $\{X^{(n)}, n = 0,1,2,3,..........\}$ where $X^{(n)}$, denotes the state of user at n[th] attempt to connect (or succeed) a call while transitioning among five states O_1, O_2, NC, C and A, at n = 0, we have

$$\left.\begin{aligned} P\left[X^{(0)} = O_1\right] &= p \\ P\left[X^{(0)} = O_2\right] &= (1-p) \\ P\left[X^{(0)} = NC\right] &= 0 \\ P\left[X^{(0)} = C\right] &= 0 \\ P\left[X^{(0)} = A\right] &= 0 \end{aligned}\right\} \quad ...(6.1)$$

Now, the transition probability matrix is

States $X^{(n)}$

$$X^{(n-1)} \begin{array}{c|ccccc} & O_1 & O_2 & NC & C & A \\ \hline O_1 & L_1 & L_1^2(1-p_A) & \{1-(L_1+L_1^2)\} & 0 & L_1^2 p_A \\ O_2 & L_2^2(1-p_A) & L_2 & \{1-(L_2+L_2^2)\} & 0 & L_2^2 p_A \\ NC & 0 & 0 & c_1 & 1-c_1 & 0 \\ C & 0 & 0 & 1-c_2 & c_2 & 0 \\ A & 0 & 0 & 0 & 0 & 1 \end{array}$$

6.2-Transition Probability Matrix [As Proposed Shukla, Tiwari And Thakur (2010)]

VII. COMPUTATION OF TRAFFIC SHARE OVER LARGE ATTEMPTS [As Defined Shukla, Tiwari And Thakur (2010)]

Suppose the number of call attempts made by user is very large and then define $\bar{P}_i = \left[\lim_{n\to\infty} \bar{P}_i^{(n)}\right]$, $i = 1,2$ which provides a measure of traffic share between two operators in terms of cyber crime prospect. The limiting value of expressions relates to the traffic shares.

Now we again separate these expression of type A, B, C and D basis.

VIII. TWO CALL INDEX BASED ANALYSIS

We defined here ratio based user index for different categories of users and it has been explained as below

PART I: INDEX FOR NON CYBER CRIME

Type A:

Index for operator O_1:

$$I_{1\,A\,NC}(O_1) = \frac{\bar{P}_{1\,A\,NC}}{\bar{P}_{1\,A\,NC} + \bar{P}_{2\,A\,NC}}$$

$$I_{1\,A\,NC}(O_1) = \frac{\left[\{1-(L_1+L_1^2)\} C_1 L_1 p\right]}{\left[\{1-(L_1+L_1^2)\} C_1 L_1 p\right] + \left[\{1-(L_2+L_2^2)\} C_1 L_2 (1-p)\right]} \quad ...(8.1)$$

Index for operator O_2:

$$I_{2\,A\,NC}(O_2) = \frac{\bar{P}_{2\,A\,NC}}{\bar{P}_{1\,A\,NC} + \bar{P}_{2\,A\,NC}}$$

$$I_{2\,A\,NC}(O_2) = \frac{\left[\{1-(L_2+L_2^2)\} C_1 L_2 (1-p)\right]}{\left[\{1-(L_1+L_1^2)\} C_1 L_1 p\right] + \left[\{1-(L_2+L_2^2)\} C_1 L_2 (1-p)\right]} \quad ...(8.2)$$

Type B:

Index for operator O_1:

$$I_{1\,B\,NC}(O_1) = \frac{\bar{P}_{1\,B\,NC}}{\bar{P}_{1\,B\,NC} + \bar{P}_{2\,B\,NC}}$$

$$I_{1\,B\,NC}(O_1) = \frac{\left[\{1-(L_1+L_1^2)\} C_1 (1-p) \{L_1.L_2^3 (1-p_A)\}\right]}{\left[\{1-(L_1+L_1^2)\} C_1 (1-p) \{L_1 L_2^3 (1-p_A)\}\right] + \left[\{1-(L_2+L_2^2)\} C_1 p \{L_1^3 L_2 (1-p_A)\}\right]} \quad ...(8.3)$$

Index for operator O_2:

$$I_{2\,B\,NC}(O_2) = \frac{\bar{P}_{2\,B\,NC}}{\bar{P}_{1\,B\,NC} + \bar{P}_{2\,B\,NC}}$$

$$I_{2\,B\,NC}(O_2) = \frac{\left[\{1-(L_2+L_2^2)\} C_1 p \{L_1^3 L_2 (1-p_A)\}\right]}{\left[\{1-(L_1+L_1^2)\} C_1 (1-p) \{L_1 L_2^3 (1-p_A)\}\right] + \left[\{1-(L_2+L_2^2)\} C_1 p \{L_1^3 L_2 (1-p_A)\}\right]} \quad ...(8.4)$$

Type C:

Index for operator O_1:

$$I_{1\,C\,NC}\left(O_1\right)=\frac{\overline{P}_{1\,C\,NC}}{\overline{P}_{1\,C\,NC}+\overline{P}_{2\,C\,NC}}$$

$$I_{1\,C\,NC}\left(O_1\right)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1 p\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1 p\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1\left(1-p\right)\right]}\text{...(8.5)}$$

Index for operator O_2:

$$I_{2\,C\,NC}\left(O_2\right)=\frac{\overline{P}_{2\,C\,NC}}{\overline{P}_{1\,C\,NC}+\overline{P}_{2\,C\,NC}}$$

$$I_{2\,C\,NC}\left(O_2\right)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1\left(1-p\right)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1 p\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1\left(1-p\right)\right]}\text{...(8.6)}$$

Type D:

Index for operator O_1:

$$I_{1\,D\,NC}\left(O_1\right)=\frac{\overline{P}_{1\,D\,NC}}{\overline{P}_{1\,D\,NC}+\overline{P}_{2\,D\,NC}}$$

$$I_{1\,D\,NC}\left(O_1\right)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1\left(1-p\right)L_2^3\left(1-p_A\right)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1\left(1-p\right)L_2^3\left(1-p_A\right)\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1 p L_1^3\left(1-p_A\right)\right]}\text{...(8.7)}$$

Index for operator O_2:

$$I_{2\,D\,NC}\left(O_2\right)=\frac{\overline{P}_{2\,D\,NC}}{\overline{P}_{1\,D\,NC}+\overline{P}_{2\,D\,NC}}$$

$$I_{2\,D\,NC}\left(O_2\right)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1 p L_1^3\left(1-p_A\right)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}C_1\left(1-p\right)L_2^3\left(1-p_A\right)\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}C_1 p L_1^3\left(1-p_A\right)\right]}\text{...(8.8)}$$

PART II: INDEX FOR CYBER CRIME:

Type A:

Index for operator O_1:

$$I_{1\,A\,CC}\left(O_1\right)=\frac{\overline{P}_{1\,A\,CC}}{\overline{P}_{1\,A\,CC}+\overline{P}_{2\,A\,CC}}$$

$$I_{1\,A\,CC}\left(O_1\right)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)L_1 p\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)L_1 p\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)L_2\left(1-p\right)\right]}\text{...(8.9)}$$

Index for operator O_2:

$$I_{2\,A\,CC}\left(O_2\right)=\frac{\overline{P}_{2\,A\,CC}}{\overline{P}_{1\,A\,CC}+\overline{P}_{2\,A\,CC}}$$

$$I_{2\,A\,CC}\left(O_2\right)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)L_2\left(1-p\right)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)L_1 p\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)L_2\left(1-p\right)\right]}\text{...(8.10)}$$

Type B:

Index for operator O_1:

$$I_{1\,B\,CC}\left(O_1\right)=\frac{\overline{P}_{1\,B\,CC}}{\overline{P}_{1\,B\,CC}+\overline{P}_{2\,B\,CC}}$$

$$I_{1\,B\,CC}\left(O_1\right)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)\left(1-p\right)\left\{L_1L_2^3\left(1-p_A\right)\right\}\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)\left(1-p\right)\left\{L_1L_2^3\left(1-p_A\right)\right\}\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)p\left\{L_1^3L_2\left(1-p_A\right)\right\}\right]}\text{...(8.11)}$$

Index for operator O_2:

$$I_{2\,B\,CC}\left(O_2\right)=\frac{\overline{P}_{2\,B\,CC}}{\overline{P}_{1\,B\,CC}+\overline{P}_{2\,B\,CC}}$$

$$I_{2\,B\,CC}\left(O_2\right)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)p\left\{L_1^3L_2\left(1-p_A\right)\right\}\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}\left(1-C_1\right)\left(1-p\right)\left\{L_1L_2^3\left(1-p_A\right)\right\}\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}\left(1-C_1\right)p\left\{L_1^3L_2\left(1-p_A\right)\right\}\right]}\text{...(8.12)}$$

Type C:

Index for operator O_1:

$$I_{1\,C\,CC}(O_1)=\frac{\bar{P}_{1\,C\,CC}}{\bar{P}_{1\,C\,CC}+\bar{P}_{2\,C\,CC}}$$

$$I_{1\,C\,CC}(O_1)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)\,p\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)\,p\right]+\left[\left\{1-\left(L_1+L_2^2\right)\right\}(1-C_1)(1-p)\right]} \quad ...(8.13)$$

Index for operator O_2:

$$I_{2\,C\,CC}(O_2)=\frac{\bar{P}_{2\,C\,CC}}{\bar{P}_{1\,C\,CC}+\bar{P}_{2\,C\,CC}}$$

$$I_{2\,C\,CC}(O_2)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}(1-C_1)(1-p)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)\,p\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}(1-C_1)(1-p)\right]} \quad ...(8.14)$$

Type D:

Index for operator O_1:

$$I_{1\,D\,CC}(O_1)=\frac{\bar{P}_{1\,D\,CC}}{\bar{P}_{1\,D\,CC}+\bar{P}_{2\,D\,CC}}$$

$$I_{1\,DCC}(O_1)=\frac{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)(1-p)L_2^3(1-p_A)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)(1-p)L_2^3(1-p_A)\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}(1-C_1)\,pL_1^3(1-p_A)\right]} \quad ...(8.15)$$

Index for operator O_2:

$$I_{2\,D\,CC}(O_2)=\frac{\bar{P}_{2\,D\,CC}}{\bar{P}_{1\,D\,CC}+\bar{P}_{2\,D\,CC}}$$

$$I_{2\,DCC}(O_2)=\frac{\left[\left\{1-\left(L_2+L_2^2\right)\right\}(1-C_1)\,pL_1^3(1-p_A)\right]}{\left[\left\{1-\left(L_1+L_1^2\right)\right\}(1-C_1)(1-p)L_2^3(1-p_A)\right]+\left[\left\{1-\left(L_2+L_2^2\right)\right\}(1-C_1)\,pL_1^3(1-p_A)\right]} \quad ...(8.16)$$

IX. SIMULATION STUDY

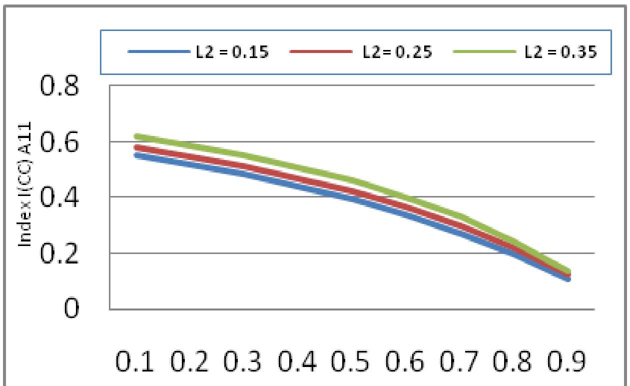

Fig.1.1 Blocking Probability L1
(When C1= 0.3, p=0.15, pA=0.2)

In light of figure 1.1 it is observe that for the constant value of C_1= 0.3, p=0.15 and p_A=0.2 index curve of cyber crime users is in downward trend for the little increment of opponent blocking by L_2=0.10.

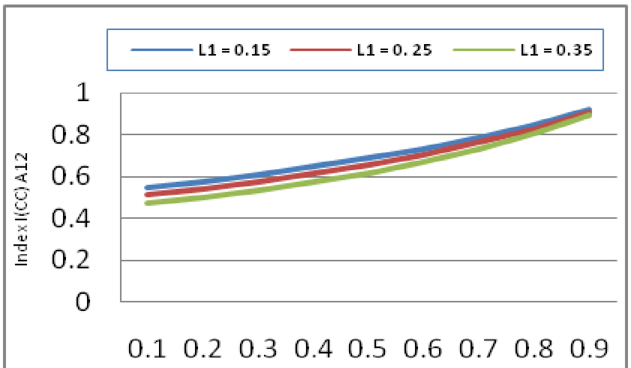

Fig.1.2 Blocking Probability L2
(When C1= 0.2, p=0.25, p_A=0.3)

In view of figure 1.2 it is clear that for the little increment of blocking probability L_2 index curve of cybercrime based users is in upward trend for the fixed value of C_1= 0.2, p=0.25and p_A=0.3 with respect to varying increment of blocking probability of opponent operator.

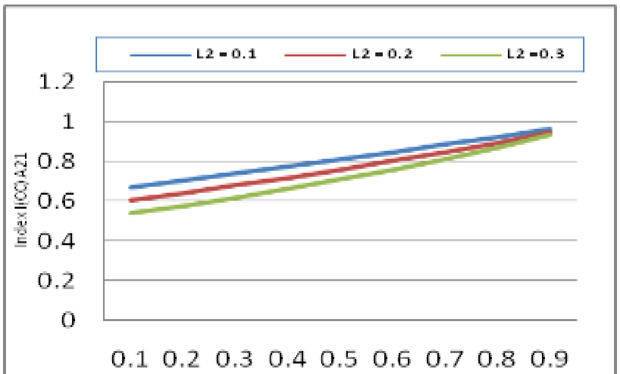

Fig.1.3 Blocking Probability L1
(When C1= 0.35, p=0.3, pA=0.1)

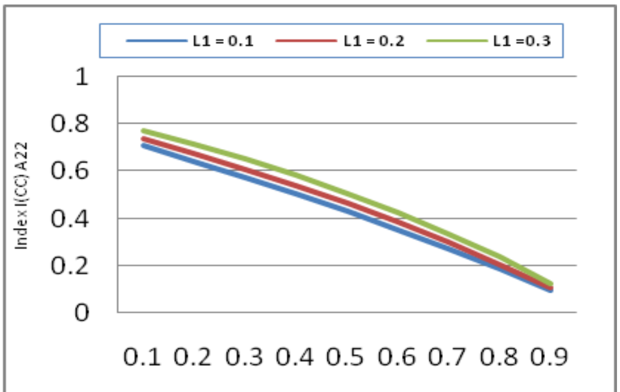

Fig.1.4 Blocking Probability L2
(When C1= 0.15, p=0.25, pA=0.15)

While looking in fig. 1.3 it is observe that for increasing values of L_1 and for fixed value of $C_1=0.35$ maximum index value is covered and it is nearly 1 while in fig. 1.4 index value is nearly 80 percent for some prefixed network parameter.

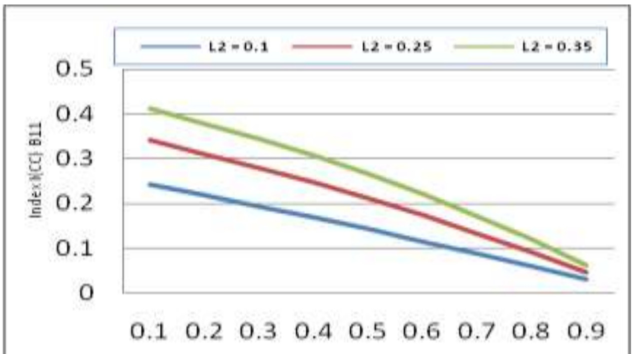

Fig.1.5 Blocking Probability L1
(When C1= 0.15, p=0.2, pA=0.25)

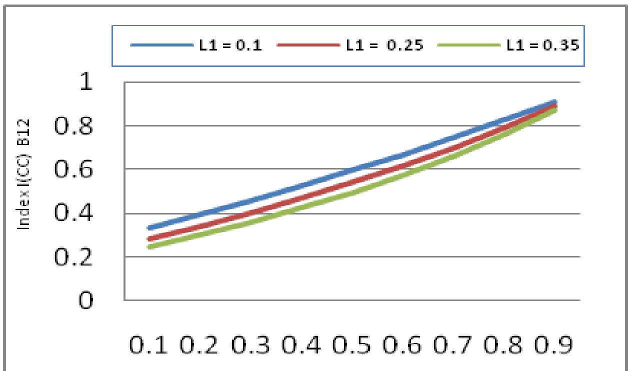

Fig.1.6 Blocking Probability L2
(When C1= 0.25, p=0.3, pA=0.15)

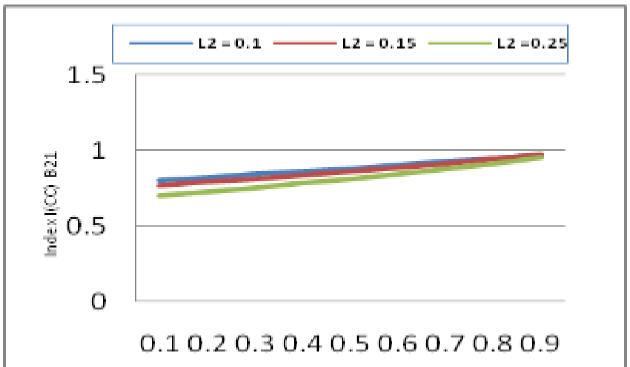

Fig.1.7 Blocking Probability L1
(When p= 0.15, pA=0.3, C1=0.2)

As shown in fig. 1.5 it is found that maximum index value is nearly 40 percent for prefixed $p_A=0.25$,$C_1= 0.15$ and p=0.2 while in fig.1.6 and 1.7 show increasing pattern with the little increment of opponent blocking and some fixed network parameter.

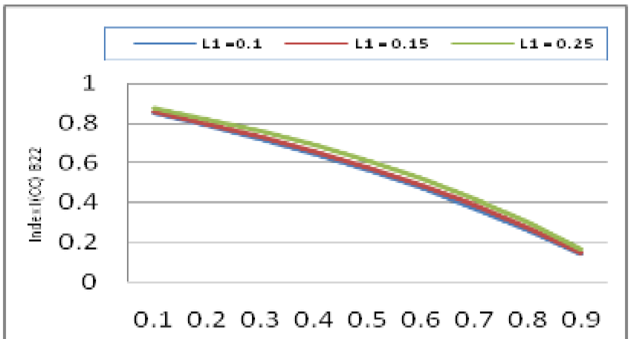

Fig.1.8 Blocking Probability L1
(When C1= 0.25, p=0.1, pA=0.35)

In fig.1.8 it reflect that for constant parameter $C_1=$ 0.25, $p_A=0.35$ & p=0.1 index curve is in downward trend.

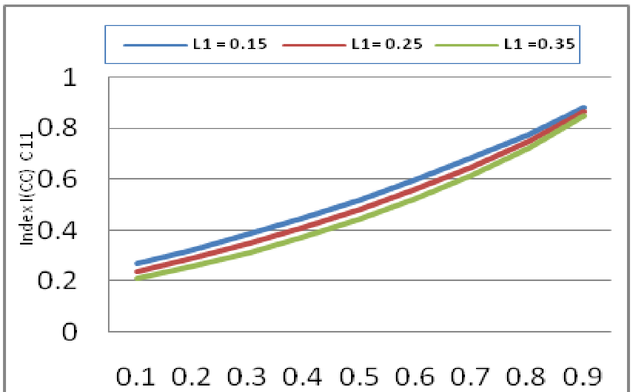

Fig.1.9 Blocking Probability L2
(When c1= 0.2, p=0.25, pA=0.35)

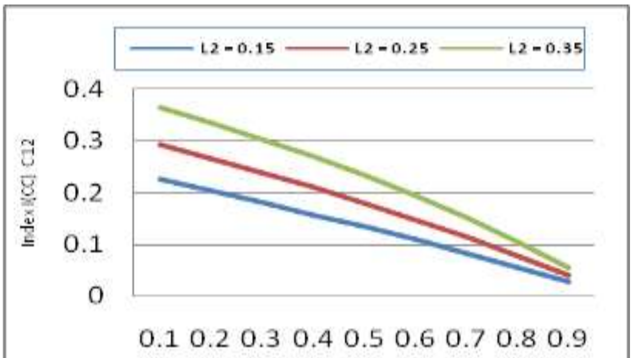

Fig.1.10 Blocking Probability L1
(When pA= 0.3, C1=0.25, p=0.15)

In fig 1.9 index shows upward trend for some increasing value of L_1 and it is clear from fig. 1.10 index value is restricted in some reason with constant value of $p=0.15, p_A= 0.3, C_1=0.25$.

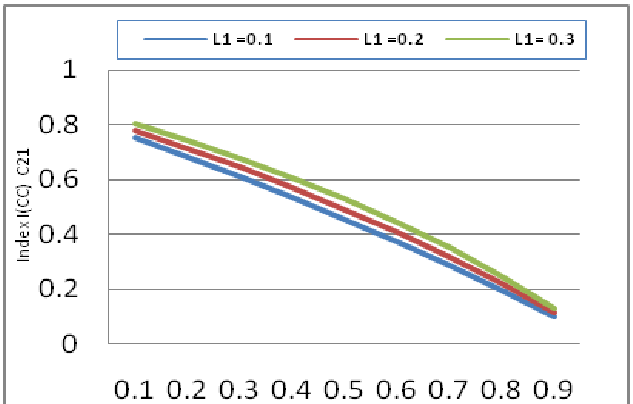

Fig.1.11 Blocking Probability L2
(When c1= 0.15, p=0.2, pA=0.15)

In light of fig.1.11 similar pattern seen as in figure 1.8.

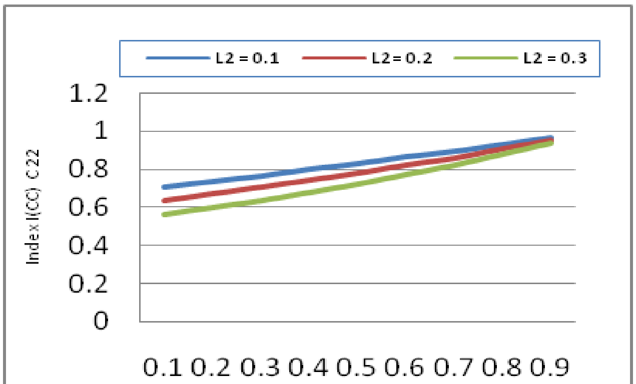

Fig.1.12 Blocking Probability L1
(When pA= 0.05, C1=0.3, p=0.25)

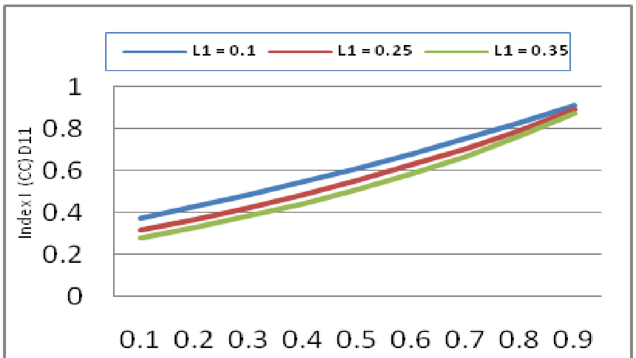

Fig.1.13 Blocking Probability L2
(When p= 0.35, pA=0.25, C1=0.1)

As soon in fig. 1.12 same pattern as fig. 1.3 appears for prefixed network parameter and increasing value of opponent blocking. In figure 1.13 it is clear that index of cyber crime users increase with respect to fixed value of $p_A=0.25$, $C_1=0.1$ and $p= 0.35$.

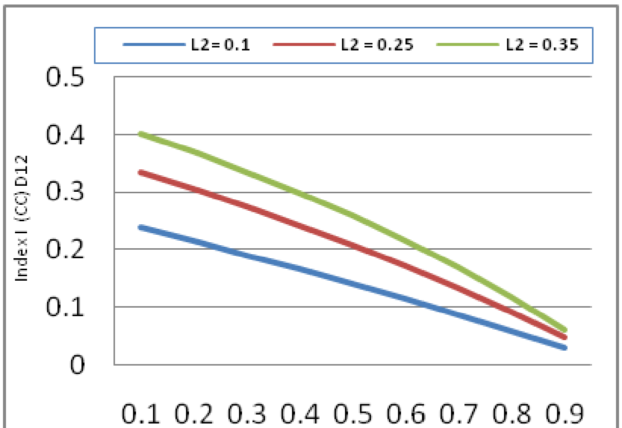

Fig.1.14 Blocking Probability L1
(When C1= 0.15, p=0.2, pA=0.3)

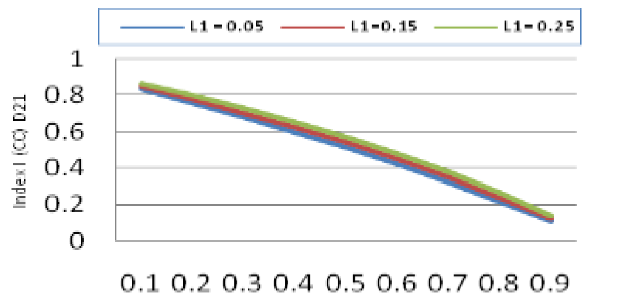

Fig.1.15 Blocking Probability L2
(When p= 0.1, pA=0.2, C1=0.35)

In view of fig. 1.14 it to be seems that cyber crime based user index with constant increment of L_2 and for fixed value of C_1= 0.15, p=0.2 and p_A=0.3 is restricted in nearly 40 percentage while Fig. 1.15 shows that index curve are overlapped at different stage of blocking.

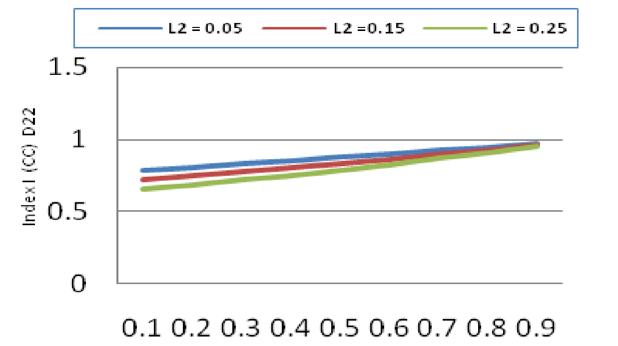

Fig.1.16 Blocking Probability L1
(When C1= 0.15, p=0.2, pA=0.25)

While looking in fig.1.16 it is observe that index shows upward trend with the little increment of opponent blocking L_2 by o.10 and when C_1= 0.15, p=0.2 and $p_{A=}$0.25,Index graph reaches nearly to1 subject to the condition for increasing value of L_1.

X. CONCLUSION

Indexing technique plays an important role for the prediction of behaviour of cyber criminals specially in two-call basis setup. Index formations of different categories are clearly indicated for the visibility of probability based study of user behaviour. At C_1=0.15 cyber crime user index approaches nearly to 1 subject to the condition when p=0.2 and p_A=0.25 whereas at C_1=0.35 pattern found to be overlapped of different stage of opponent blocking for p_A=0.2, and p= 0.1. Moreover one can conclude that ratio based user index clearly justify the probability based evaluation of the behaviour of cyber crime based users in case of internet traffic sharing for different stage of network blocking in two-call based setup.

REFERENCES

[1] Francini, A. and Chiussi, F.M. (2002): Providing QoS guarantees to unicast and multicast flows in multistage packet switches, IEEE Selected Areas in Communications, vol. 20, no. 8, pp. 1589-1601.

[2] Medhi, J.(1991): Stochastic Processes, Wiley Eastern Limited (Fourth reprint), New Delhi.

[3] Naldi, M. (2002): Internet access traffic sharing in a Multi-operator environment, Computer Networks, Vol. 38, pp.809-824.

[4] Dorea, C.C.Y., Cruz and Rojas, J. A. (2004): Approximation results for non-homogeneous Markov chains and some applications, Sankhya, Vol. 66, Issue No. 02, pp. 243-252.

[5] Shukla, D., Gadewar, S. and Pathak, R.K. (2007): A stochastic model for space division switches in computer networks, international journal of applied mathematics and computation, Elsevier journals, Vol. 184, Issue No. 02, pp235-269.

[6] Shukla, D. and Thakur, Sanjay, (2007): Crime based user analysis in internet traffic sharing under cyber crime, Proceedings of National Conference on Network Security and Management (NCSM-07), pp. 155-165.

[7] Agarwal, Rinkle and Kaur, Lakhwinder (2008): On reliability analysis of fault-tolerant multistage interconnection networks, international journal of computer science and security (IJCSS) Vol. 02, Issue No. 04, pp. 1-8.

[8] Shukla, D., Jain, Saurabh and Ojha , Shweta (2010) : Deadlock index analysis of multi-level queue scheduling in operating system using data model approach, International Journal of Computer Science and Telecommunication ,Vol 6, no 29, pp 93-110.

[9] Tiwari, Virendra, Thakur, Sanjay and Shukla, D.(2010):Cyber crime analysis for multi-dimensional effect in computer network, Journal of Global Research in Computer Science, Vol.1, no. 4., pp 31-37.

[10] M. Naldi (1999): Measurement based modelling of Internet Dial-up Access Connections, Computer Networks, vol. 31, issue 22, pp. 2381-2390.

[11] Shukla, D., Thakur, Sanjay (2009): State Probability Analysis of Users in Internet between two Operators, international journal of advanced networking and applications (IJANA), 2009 vol. 1, issue 2, pp. 90-95.

[12] Shukla, D., Tiwari, M.,Thakur, S. Tiwari,V.(2009): Rest state analysis in internet traffic distribution in multi-operator environment, research journal of management and information technology (GNIM's), vol 1 issue 1, pp. 72-82.

[13] Shukla, D., Tiwari, M.,Thakur, S. Deshmukh,A.(2009): Share loss analysis of internet traffic distribution in computer networks, international journal of computer science and security (IJCSS), vol 3, Issue 4, pp. 414-427.

[14] Shukla, D.,Gadewar, Surendra (2007):Stochastic model for cell movement in a knockout switch in computer networks, journal of high speed network, vol.16, no.3, pp. 310-332.

[15] Shukla, D. Gadewar, S. Pathak, R.K.,(2007): A Stochastic Model for Space-Division Switches in Computer Networks, Applied Mathematics and Computation (Elsevier Journal), vol. 184, Issue 2, pp. 235-269.

[16] D. Shukla, V. Tiwari, A. Kareem P and S. Thakur (2010): Effects of Disconnectivity Analysis for Congestion Control in Internet Traffic Sharing, vol. 18, no. 1, pp. 37-46.

[17] Shukla, D. and Thakur, Sanjay (2010): Index based internet traffic sharing analysis of users by a markov chain probability model,

Karpagam Journal of Computer Science, Vol. 4, No. 3, pp. 1539-1545.

[18] Thakur, Sanjay and Shukla, D. (2010): Iso-share analysis of internet traffic sharing in presence of favoured dis-connectivity, Computer science and Telecommunication, Vol. 27, No.4, pp. 16-22.

[19] Shukla, D. and Singhai, Rahul (2011): Analysis of user web browsing behaviour using Markov chain model, international journal of advanced networking and application (IJANA), Vol. 2, No. 5, pp. 824-830.

[20] Shukla, D.,Gangele, Sharad, Singhai, R., Verma, Kapil (2011): Elasticity analysis of web-browsing behaviour of users, international journal of advanced networking and application(IJANA), Vol. 3 No.3, pp. 1162-1168.

[21] Shukla, D., Gangele, Sharad, Verma, kapil and Singh, Pankaja (2011a): Elasticity of Internet Traffic distribution in Computer network in two-market environment, Journal of Global Research in Computer Science (JGRCS), Vol. 2, No.6, pp. 6-12.

[22] Shukla, D., Gangele , Sharad, Verma, Kapil and Singh, Pankaja (2011b): Elasticity and Index analysis of usual Internet traffic share problem, international journal of advanced research in computer science (IJARCS), Vol. 02, No. 04, pp. 473- 478.

[23] Shukla, D., Verma, Kapil and Gangele, Sharad, (2012a): Curve Fitting Approximation In Internet Traffic Distribution In Computer Network In Two Market Environment, international journal of computer science and information security (IJCSIS), Vol. 10, Issue 05, pp. 71-78.

[24] Shukla, D., Verma, Kapil and Gangele, Sharad, (2012b): Least Square Fitting Applications under Rest State Environment in Internet Traffic Sharing in Computer Network, International Journal of Computer Science and Telecommunications (IJCST), Vol.3, Issue 05, pp.43-51.

[25] Shukla, D., Verma, Kapil, Dubey, Jayant and Gangele, Sharad (2012c): Cyber Crime Based Curve Fitting Analysis in Internet Traffic Sharing in Computer Network. International journal of computer application (IJCA), Vol.46 No.22, pp. 41-51.

[26] Shukla, D., Verma, Kapil, Bhagwat, Shree and Gangele, Sharad (2012d): Curve Fitting Analysis of Internet Traffic Sharing Management in Computer Network under Cyber Crime, International journal of computer application (IJCA), Vol. 47, No. 24, pp. 36-43.

[27] Gangele, S. Verma, K. and Shukla, D., (2014a): Bounded Area Estimation of Internet Traffic Share Curve, International Journal of Computer Science and Business Informatics, Vol. 10, No. 1, pp. 54-67.

[28] Gangele,Sharad,Dongre,Ashish(2014b):Probability density estimation function of browser share curve for users web browser behaviour, International journal of engineering research and development, Vol. 10, Issue 6,pp.31-41.

[29] Gangele,Sharad,Shukla,D.,(2014c):Area computation of internet traffic share problem with special reference to cyber crime environment, International journal of computer networks and wireless communication, Vol. 4,no. 3,pp.208-219.