Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Internet Traffic Distribution Management under Cyber Crime Marketing Plans

***SANJAY THAKUR, **SAURABH JAIN, ***VIRENDRA TIWARI, ****DIWAKAR SHUKLA**

**Associate Professor, Department of Computer Science and Engineering, Lord Krishna College of Technology, Indore, MP, INDIA*

*** Associate Professor, Department of MCA, Shri Vaishnav[SM] Institute of Technology & Science, Indore (M.P.), INDIA*

****Associate Professor, Lakshmi Narain College of Technology, Bhopal, (M.P.), INDIA*

*****Associate Professor, Department of Mathematics and Statistics, Dr. H.S.G. Central University, Sagar, MP, INDIA*

ABSTRACT: Today, the need of Internet is growing in every moment. A breed of cyber criminals is also emerging in parallel for generating an environment of cyber crimes. The cyber crime begins after the connection with an operator on the network. This paper use the Markov chain model to analysis the effect of blocking probability, initial share and cyber crime probabilities on the traffic distribution between the operators under two cyber crime marketing plans. Users are grouped into cyber criminals and non-cyber criminals. Further, cyber criminals are regrouped into serious (or hardcore) and non-serious. Model based analysis is focused on to know the crime impact over user groups during traffic sharing. The users access the Internet on call-by-call basis between the ISPs. Operators who promote cyber crime as marketing plans (AOP and SOP) can get better share of traffic.

General Terms

Internet traffic, User Behaviour, Stochastic analysis.

Keywords: Markov Chain Model, Initial Preference, Blocking Probability, Call-by-Call basis, Traffic Share, Cyber Criminals, Transition Probability Matrix.

I. INTRODUCTION

In computer networking due to the congestion network users either make repeated attempts on same operator or change his choice of the operator on a call-by-call basis. The traffic shares between operators determine the first choice and quality of service of operators. Naldi [2] has suggested Markov Chain model for the analysis of Internet Access Traffic sharing in a Multi Operator Environment. This model uses to analysis the effect of blocking probability and initial preference on the traffic distribution between the operators. In current day broadband service is widely used for accessing the internet. But dial-up service for Internet access is still use through PSTN, which use a modem to connect to the Internet. It is assumed that each user's first choice is affected by marketing plans after user choice shift to another operator for the successive calls while first call attempt is failed.

This paper is extending part of Shukla et al [5] have discussed stochastic modeling of Internet traffic management. Dorea et al. [1] used Markov chain for the modelling of a system and derived some useful approximations. Shukla et al. [16] studied cyber crime based curve fitting analysis in internet traffic sharing in computer network. The contributions of Shukla et al. [4], [6], [8], [9], [11], [12], [13], [14], [15] Shukla and thakur [7], [10], Newby and Dagg [3] and Yeian [17] are used as helping tools to design the model.

1.1 Categorization of users

Users are categorizing as :

(i) Cyber Criminal [CC]- Who after getting success in call connection performs cyber-crime.

(ii) Non-Cyber Criminal [NC]- Who never opt to cyber-crimes on Internet the moment call gets connected. One can further sub-divide the cyber criminals into two groups as [see figure 1].

(a)Serious Cyber Criminal [SC] - Those who stick to crime for long period

(b) Non-Serious Cyber Criminal [NSC]-Those who stay for a little while over cyber crimes and then quickly come back to call as NC. A general purpose diagram of categorization and share is in Figure 2.

© 2014, IJARCSSE All Rights Reserved

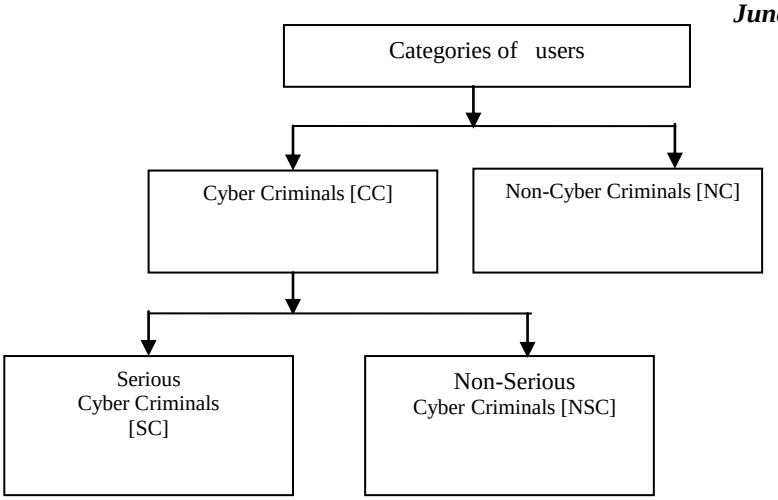
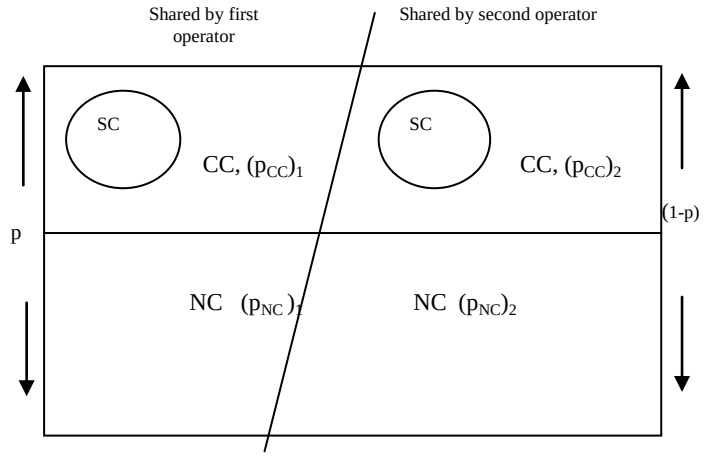


Figure 1 (Crime based Categories of user)



$p = (p_{CC})_1 + (p_{NC})_1$; $(1-p) = p_{CC})_2 + (p_{NC})_2$

Figure 2 (Crime-subdivision of user)

1.2 Marketing Plans

(A) Attract-On-Plan (AOP): where user is attracted for cyber-crime.

(B) Stay-On-Plan (SOP): where user is ensured with a kind of safety to continue with crime practice for a long. If c_1 and c_2 are probability based parameters related against to these plans then reducing c_1, c_2 would measure the effect of plans over traffic distribution.

1.3 Assumptions for User's Behaviour

- The competitive market has a café, containing Internet facility of two operators O_1 and O_2.
- A user enters into café with initial choice (first choice) p and (1-p) for O_1 and O_2 respectively, $(0 \leq p \leq 1)$.
- A successful call connection provides to user a marketing package related to cyber-crime, denoted as C, with attraction probability $(1-c_1)$ and detention probability $(1-c_2)$. The $(1-c_1)$ relates to Attract-On-Plan (AOP) and $(1-c_2)$ relates to Stay-On-Plan (SOP) of marketing.
- After each failed call attempt, the user has two choices: he can abandon with probability p_A or switch over to other operator for a new attempt.
- After a successful attempt, user has two choices: he performs cyber-crime with SOP package or can opt the usual web surfing through Internet (with probability c_1). This choice is treated as an attempt related to web connectivity.
- Attempt has two definitions as (a) Call connecting attempt and (b) Surfing attempt (occurs when call attempt is successful).
- User may come-back to usual net-surfing whenever willing (with probability c_2), or may continue with cyber crime surfing depending on attraction of SOP.
- From C, user can neither abandon nor disconnect.
- During the repeated connectivity call, the blocking probability of O_1 is L_1 and O_2 is L_2. The blocking implies the situation when call attempt process fails to connect with an operator. The figure 3 shows a relational diagram of different model parameters.

© 2014, IJARCSSE All Rights Reserved

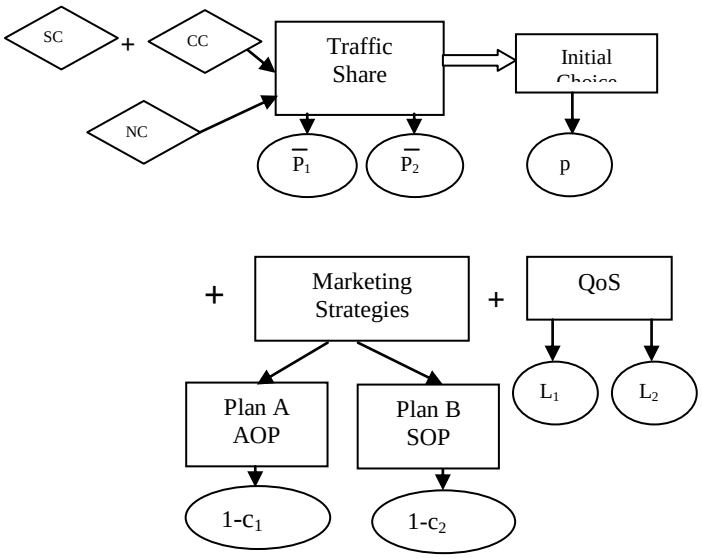


Figure 3 (Relational Diagram)

Under above assumptions, user's behavior can be modelled 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: First operator
State O_2: Second operator
State NC: Success (in connectivity) but no cyber-crime
State A: Abandon of attempt process
State C: Connectivity and cyber-crime Conduct through surfing.

The diagrammatic form of transition between two operators is given in figure 4.

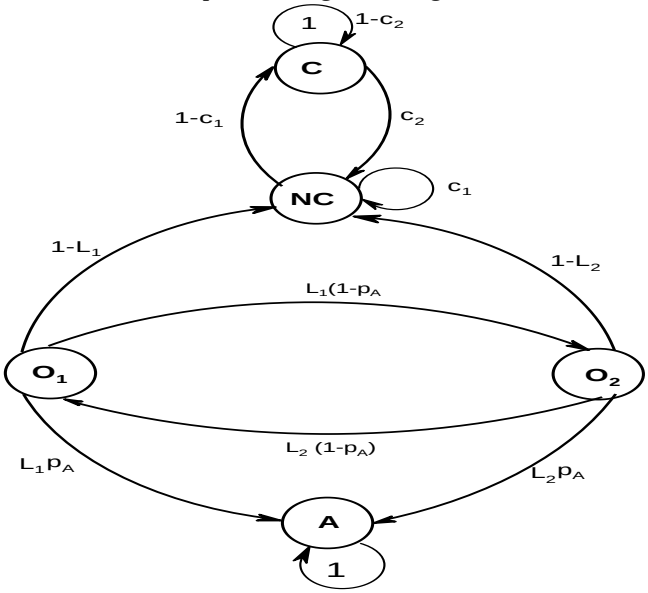


Figure 4 (Transition diagram of model)

States

$X^{(n)}$

$X^{(n-1)}$	O_1	O_2	NC	C	A
O_1	0	$L_1(1-p_A)$	$1-L_1$	0	L_1p_A
O_2	$L_2(1-p_A)$	0	$1-L_2$	0	L_1p_A
NC	0	0	c_1	$1-c_1$	0
C	0	0	c_2	$1-c_2$	0
A	0	0	0	0	1

Figure 5 (Transition probability matrix

© 2014, IJARCSSE All Rights Reserved

II. n^{th} STEP STATE PROBABILITY

Under Markov chain model, the n^{th} step state probability for O_1 and O_2 is:

$$P\left[X^{(n)} = O_1\right] = p\sqrt{(L_1 L_2)^n}\left[(1-p_A)^n\right]$$

when n even

$$P\left[X^{(n)} = O_1\right] = (1-p)L_2\sqrt{(L_1 L_2)^{n-1}}\left[(1-p_A)^n\right]$$

when n odd

$$P\left[X^{(n)} = O_2\right] = (1-p)\sqrt{(L_1 L_2)^n}\left[(1-p_A)^n\right]$$

when n even

$$P\left[X^{(n)} = O_2\right] = pL_1\sqrt{(L_1 L_2)^{n-1}}\left[(1-p_A)^n\right]$$

when n odd

III. FINAL TRAFFIC SHARE

In general, assume that a user has to make n call attempts to get his call connected with an operator O_i (i = 1, 2).. Let $[\overline{P_i}^{(n)}]$ denotes the final traffic of operator O_i after n attempts which varies over groups and attitude of users along with market and network parameters.

3.1 Traffic Share by NC

$$\left[\overline{P_1}^{(n)}\right]_{NC} = P\left[\begin{array}{l} Call\ \ complete\ \ with\ \ O_1\ and\ \ user\ is\ at \\ Non-crime\ \ state\,(NC)\ at\ \ n^{th}\ attempt \end{array}\right]$$

$$= P\left[At\ \ (n-2)^{th}\ attempt\ \ on\ \ O_1\right]$$

$$P\left[\begin{array}{l} (n-1)^{th}\ on\ NC \\ \hline (n-2)^{th}\ on\ \ O_1 \end{array}\right]$$

$$P\left[\begin{array}{l} n^{th}\ on\ NC \\ \hline (n-1)^{th}\ on\ NC \end{array}\right]$$

$$= (1-L_1)\,c_1\left[\sum_{i=0}^{n-2} P\left\{X^{(i)} = O_1\right\}\right]$$

$$\left[\overline{P_1}^{(n)}\right]_{NC}^{Even} = (1-L_1)c_1$$

$$\left[\begin{array}{l} p\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]^n}\right\} + \\ \dfrac{(1-p)L_2(1-p_A)\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]^{n-2}}\right\}}{1-L_1L_2(1-p_A)^2} \end{array}\right]$$

$$= P\left[X^{(n-2)} = O_1\right]$$

$$P\left[\begin{array}{l} X^{(n-1)} = NC \\ \hline X^{(n-2)} = O_1 \end{array}\right]$$

$$P\left[\begin{array}{l} X^{(n)} = NC \\ \hline X^{(n-1)} = NC \end{array}\right]$$

$$\left[\overline{P_1}^{(n)}\right]_{NC}^{Odd} = (1-L_1)c_1\left[p + (1-p)L_2(1-p_A)\right]$$

$$\left[\frac{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]^n}}{1-L_1L_2(1-p_A)^2}\right]$$

© 2014, IJARCSSE All Rights Reserved

3.2 Traffic share by CC

$$\left[\overline{P_1}^{(n)}\right]_{CC}^{Even} = (1-L_1)(1-c_1)\left[\begin{array}{l} p\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n}\right\}+ \\ \dfrac{(1-p)L_2(1-p_A)\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n-2}\right\}}{1-L_1L_2(1-p_A)^2} \end{array}\right]$$

$$\left[\overline{P_1}^{(n)}\right]_{CC}^{Odd} = (1-L_1)(1-c_1)\left[p+(1-p)L_2(1-p_A)\right]\left[\frac{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n}}{1-L_1L_2(1-p_A)^2}\right]$$

3 .3 Traffic Share by NSC

$$\left[\overline{P_1}^{(n)}\right]_{NSC}^{Even} = (1-L_1)(1-c_1)c_2$$

$$\left[p+(1-p)L_2(1-p_A)\right]\frac{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n-3}}{1-L_1L_2(1-p_A)^2}$$

$$\left[\overline{P_1}^{(n)}\right]_{NSC}^{Odd} = (1-L_1)(1-c_1)c_2\left[\begin{array}{l} p\left\{1-\sqrt{[L_1L_2(1-p_A)^2]}^{n}\right\}+(1-p)L_2(1-p_A) \\ \dfrac{\left\{1-\sqrt{[L_1L_2(1-p_A)^2]}^{n-3}\right\}}{1-L_1L_2(1-p_A)^2} \end{array}\right]$$

3.4 Traffic Share by SC

$$\left[\overline{P_1}^{(n)}\right]_{SC}^{Even} = (1-L_1)(1-c_1)(1-c_2)\left[p+(1-p)L_2(1-p_A)\right]\frac{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n-3}}{1-L_1L_2(1-p_A)^2}$$

$$\left[\overline{P_1}^{(n)}\right]_{SC}^{Odd} = (1-L_1)(1-c_1)(1-c_2)\left[\begin{array}{l} p\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n}\right\}+(1-p)L_2(1-p_A) \\ \dfrac{\left\{1-\sqrt{\left[L_1L_2(1-p_A)^2\right]}^{n-3}\right\}}{1-L_1L_2(1-p_A)^2} \end{array}\right]$$

IV. TRAFFIC SHARE OVER LARGE ATTEMPTS

Suppose the number of call attempts made by user is very large, and then define

$\overline{P_i} = \left[\lim_{n\to\infty} \overline{P_i}^{(n)}\right]$, $i = 1,2$

This provides a measure of traffic share between two operators in terms of cyber crime prospect. The limiting value of expressions of section 3 relates to traffic shares are:

© 2014, IJARCSSE All Rights Reserved

$$\left[\overline{P_1}\right]_{NC} = \frac{(1-L_1)c_1}{1-L_1L_2(1-p_A)^2}\left[p+(1-p)L_2(1-p_A)\right] \quad - (1)$$

$$\left[\overline{P_2}\right]_{NC} = \frac{(1-L_2)c_1}{1-L_1L_2(1-p_A)^2}\left[(1-p)+pL_1(1-p_A)\right] \quad - (2)$$

$$\left[\overline{P_1}\right]_{CC} = \frac{(1-L_1)(1-c_1)}{1-L_1L_2(1-p_A)^2}\left[p+(1-p)L_2(1-p_A)\right] \quad - (3)$$

$$\left[\overline{P_2}\right]_{CC} = \frac{(1-L_2)(1-c_1)}{1-L_1L_2(1-p_A)^2}\left[(1-p)+pL_1(1-p_A)\right] \quad - (4)$$

$$\left[\overline{P_1}\right]_{NSC} = \frac{(1-L_1)(1-c_1)c_2}{1-L_1L_2(1-p_A)^2}\left[p+(1-p)L_2(1-p_A)\right] \quad - (5)$$

$$\left[\overline{P_2}\right]_{NSC} = \frac{(1-L_2)(1-c_1)c_2}{1-L_1L_2(1-p_A)^2}\left[(1-p)+pL_1(1-p_A)\right] \quad - (6)$$

$$\left[\overline{P_1}\right]_{SC} = \frac{(1-L_1)(1-c_1)(1-c_2)}{1-L_1L_2(1-p_A)^2}\left[p+(1-p)L_2(1-p_A)\right] \quad - (7)$$

$$\left[\overline{P_2}\right]_{SC} = \frac{(1-L_2)(1-c_1)(1-c_2)}{1-L_1L_2(1-p_A)^2}\left[(1-p)+pL_1(1-p_A)\right] \quad - (8)$$

V. ANALYSIS OF TRAFFIC SHARE

Consider expressions of section 3.1-3.4 and (1)-(8) to draw graphical pattern.

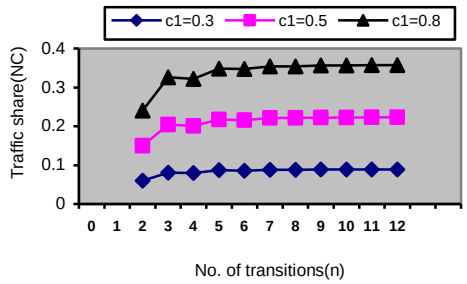


Figure 6 (p = 0.5, p_A= 0.3, L_1= 0.5, L_2 = 0.4)

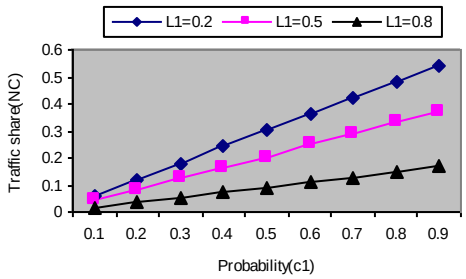


Figure 7 (p = 0.5, p_A = 0.3, L_2 = 0.4)

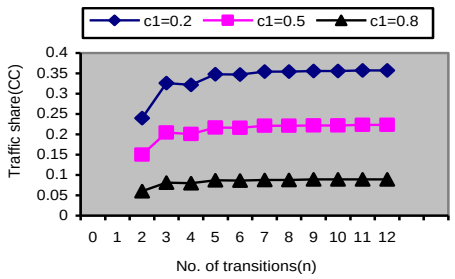


Figure 8 (p = 0.5, p_A = 0.3, L_1 = 0.5, L_2 = 0.4)

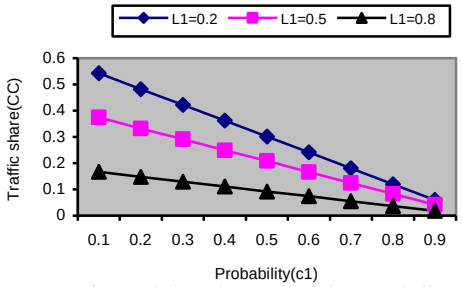


Figure 9 (p = 0.5, p_A = 0.3, L_2 = 0.6)

© 2014, IJARCSSE All Rights Reserved

In view of figure 6 and 7, it is clear that the traffic sharing by NC group has a linear relation over the increasing c_1.

With reference to figure 8 and 9, the rising value of $(1\text{-}c_1)$ has strong effect for direct increase in traffic of CC group. Define two indices for CC-group of users:

$$[I(CC)]_A = [\overline{P_1}]_{CC} / [\overline{P_1}]_{NC} = \frac{1-c_1}{c_1}$$

$$[I(CC)]_B = [\overline{P_1}]_{CC} / [\overline{P_1}]_{CC} = \frac{1-L_1}{1-L_2}$$

When $c_1 = 0.5$, $[\overline{P_1}]_{CC} = [\overline{P_1}]_{NC}$ and $[I(CC)]_A = 1$ which means the O_1 has equal proportion of cyber and non-cyber criminals into final traffic share. When $c_1 > 0.5$, the cyber criminals proportion of O_1 reduces with respect to NC group. In contrary, when $c_1 < 0.5$, the O_1 bears a large group of crime users.

In connection to specific sub-group SC of CC, as shown in figure 10 and 11 the rising crime transition probability $(1\text{-}c_1)$ increases the traffic of SC group for operator O_1 over the increasing number of attempts. The SC proportion, actually relates to $(1\text{-}c_2)$ parameter which is a part of different marketing strategy.

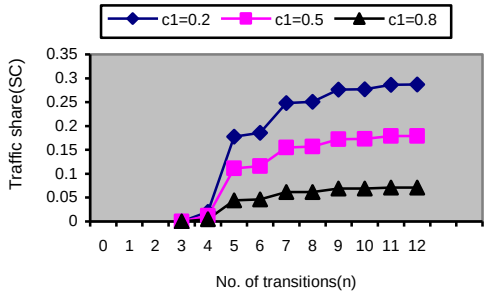


Figure 10 ($p = 0.5$, $p_A = 0.3$, $L_1 = 0.5$, $L_2 = 0.4$, $c_2 = 0.3$)

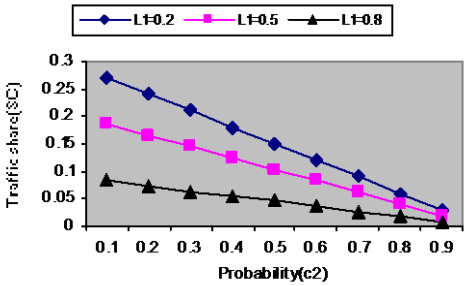


Figure 11 ($p = 0.5$, $p_A = 0.3$, $L_2 = 0.6$, $c_1 = 0.5$)

The increase in $(1\text{-}c_2)$ probability improves constantly the proportion of SC group of users which means $(1\text{-}c_2)$ has a linear relation with SC traffic. A thumb rule approximation could be $SC \approx (1\text{-}c_2)\ L_1$ and $SC \approx (1\text{-}c_2)\ L_2$.

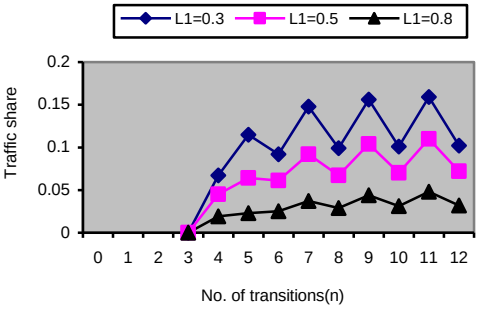


Figure 12 ($p = 0.5$, $p_A = 0.3$, $L_2 = 0.6$, $c_1 = 0.5$)

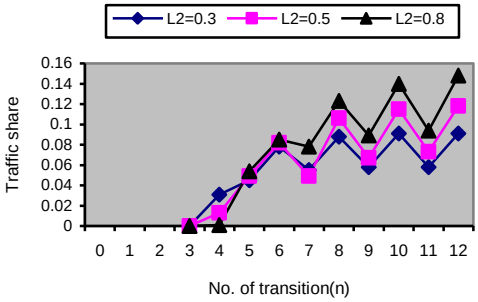


Figure 13 ($p = 0.5$, $p_A = 0.3$, $L_1 = 0.4$, $c_1 = 0.2$)

© 2014, IJARCSSE All Rights Reserved

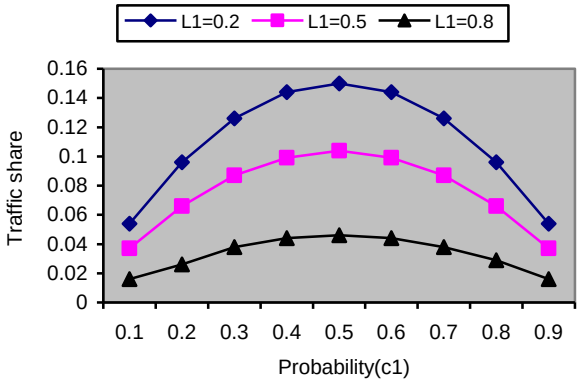


Figure 14 ($p = 0.5$, $p_A = 0.3$, $L_2 = 0.6$)

The group of users who is not hardcore in terms of performing cyber crime, the traffic share by them is affected due to variation in c_1 transition probability. For the users of the category NSC, the variation pattern of crime transition probability ($1-c_1$) and traffic sharing are in fluctuating form. (figure 12 and 13).
When self blocking probability L_1 bears higher then O_1 suffers a loss of NC, CC, SC and NSC group but for high L_2 it gains proportion. The operator O_1 has to keep his blocking probability lower than the competitor.
The little increases in c_1 produces increase in traffic but high value of c_1, reduces this traffic as shown in figure 14. At the optimum point $c_1 = 0.5$, the maximum traffic share is produced for NSC group.

VI. CONCLUSION

Providing cyber-crime facilities to the users as a marketing plan and by the reducing self network blocking, an operator can improve upon his traffic. The AOP and SOP marketing have positive role in uplifting the traffic distribution in favour of an operator. The operator O_1 gains better share than O_2 if AOP is adopted. The plan SOP which reduces c_2 has an impact to improve upon the proportion of hardcore cyber criminals. The marketing plan AOP converts NC group to CC and CC users convert into SC group with a faster rate if ($1-c_1$) increases. For further growth of SC, O_1 has to keep low blocking level in his network. With increase in ($1-c_1$) probability there is a growth of in proportion of in NSC users.

ACKNOWLEDGEMENT

Authors are thankful to the referee for critical comments and useful suggestions which has improved the quality of the revised manuscript.

REFERENCES

[1] 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.
[2] Naldi M. 2002. Internet Access Traffic sharing in a Multi Operator Environment, Computer Network, Vol. 38, pp. 809-824.
[3] Newby, M. and Dagg, R. 2002. Optical inspection and maintenance for stochastically deteriorating systems: average cost criteria, Jour. Ind. Statistical Associations Vol. 40, Issue No. 02, pp. 169-198.
[4] Shukla, D., Thakur S. and Tiwari V. 2011. Analysis of Internet Traffic Distribution for User Behaviour based Probability in Two-Market Environment in International Journal of Computer Applications, Vol. 30, No. 8, pp. 44-51.
[5] Shukla, D., Thakur S. and Tiwari V. 2010. Stochastic modeling of Internet Traffic Management in International Journal of the Computer, the Internet and Management, Vol. 18, No. 2, pp. 48-54.
[6] Shukla, D., Tiwari V., Abdul Kareem P and Thakur S. 2010. Effects of Disconnectivity Analysis for Congestion Control in Internet Traffic Sharing published in International Journal of the Computer, the Internet and Management, Vol. 18, No. 1, pp. 37-46.
[7] Shukla, D. and Thakur S. 2010. Iso-Share Analysis of Internet Traffic Sharing in the Presence of Favoured Disconnectivity in Computer Sciences and Telecommunications International Georgian Electronic Scientific Journal, No. 4(27), pp.16-22
[8] Shukla, D., Tiwari V. and Abdul Kareem P 2009. All comparison analysis in Internet traffic sharing using Markov chain model in computer networks In International Journal of Georgian Electronic Scientific Journal, Computer Science and Telecommunications-09, Vol. 6, issue 23, pp. 108-115.
[9] Shukla, D., Thakur S., Tiwari V. and Tiwari M. 2009. A comparison of methods for Internet traffic sharing in computer network In International Journal of Advanced Networking and Applications (IJANA), Vol. 1, issue 3, pp. 164-169.
[10] Shukla, D. and Thakur S. 2009. State Probability Analysis of Users in Internet between two Operators in International Journal of Advanced Networking and Applications (IJANA), Vol. 1, issue 1, pp. 90-95.

© 2014, IJARCSSE All Rights Reserved

[11] Shukla, D., Thakur S., Tiwari V. and Deshmukh A. 2009. Share Loss Analysis of Internet Traffic Distribution in Computer Networks, in International Journal of Computer Science and Security (IJCSS), Vol 3, Issue 5, pp. 414-427.

[12] Shukla, D., Verma, Kapil and Gangele, Sharad 2012. Iso-Failure in Web Browsing using Markov Chain Model and Curve Fitting Analysis, International Journal of Modern Engineering Research(IJMER) , Vol. 02, Issue 02, pp. 512-517.

[13] Shukla, D., Verma, Kapil and Gangele, Sharad 2012. Least Square Curve Fitting in Internet Access Traffic Sharing in Two Operator Environment, International Journal of Computer Application (IJCA), Vol.43(12),pp. 26-32.

[14] Shukla, D., Verma, Kapil and Gangele, Sharad 2012. Least Square Curve Fitting Applications under Rest State Environment in Internet Traffic Sharing in Computer Network, International Journal of Computer Science and Telecommunications (IJCST), Vol. 03, Issue 05.

[15] Shukla, D., Verma, Kapil and Gangele, Sharad 2012. 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.

[16] Shukla, D., Verma, Kapil, Dubey, Jayant and Gangele, Sharad 2012. Cyber crime Based Curve Fitting Analysis in Internet Traffic Sharing in Computer Network, International Journal of Computer Application (IJCA), Vol.46(22), pp. 41-51.

[17] Yeian, C. and Lygeres, J. 2005.Stabilization of class of stochastic differential equations with Markovian.

© 2014, IJARCSSE All Rights Reserved