Chapter 6

Computing the Spreading Power of a Business Portal to Propagate the Malicious Information in the Network

Hemraj Saini
Orissa Engineering College, India

Bimal Kumar Mishra
Birla Institute of Technology, MESRA, India

T. C. Panda
Orissa Engineering College, India

ABSTRACT

This paper predicts the malicious object prone site from the set of multi business portals of an organization or company. Graph theory is used to solve this problem as the diverted traffic of customers is interdependent among all the business portals. At first the interconnected business portals are represented in the form of a graph and its corresponding adjacency matrix. Later the centrality and eigenvectors were computed to find the degree of a business portal to propagate the malicious information, helping to cure the business portal by taking available security measures to avoid further infection.

1. INTRODUCTION

Business portals (Dias, 2001; Collins, 2001) are the main concern of today’s fast growing online business for almost all the sectors. These business portals are sometime suffer from the congestion due to their heavy access by the customers. To solve such a problem alternate portals are to be provided by the concern business organization/company i.e. www.indianrail.gov.in is the well known business portal of Indianrail to provide e-ticket or other facilities to its customers. But sometime due to heavy traffic of its customers it faces the problem of congestion. To solve this problem Indianrail provides the alternate business portal named www.irctc.com to divert some of its
customers. This concept or method is misused by the attackers (Mishra & Saini, 2009; Ranjan, Swaminathan, Uysal, Nucci, & Knightly, 2009; Ignacio, Matinez-Moyano, Conrad, Andersen, & Stewart, 2008) to attack the customer’s valuable information. Generally, attackers flood unnecessary traffic (Saini & Saini, 2006) towards the main business site i.e. www.indianrail.gov.in and hence it faces the problem of congestion. Due to this congestion the original traffic divert towards its alternate business portal i.e. www.irctc.com which is already hacked and prone to malicious attack by some means (Anti-Phishing Working Group, 2004; Drake, Oliver, & Koontz, 2004) of attackers as shown in Figure 1.

Such types of situation occur when an organization is not able to handle its business transaction on a single business portal. In this condition they create different other alternate business portals and hence it leads to the above mentioned situation. To detect the maximum possibility of a portal to be malicious attack prone is the main assignment of this manuscript which is handled by using graph theory (Wang & Daniels, 2008; Harju, 2007). At first the interconnected business portals are represented in the form of a graph and its corresponding adjacency matrix. Later the Centrality and eigenvectors has been calculated to find the degree of a business portal to propagate the malicious information. Computation of the degree of a business portal to propagate the malicious information helps to cure the business portal by taking available security measures to avoid the further infection.

2. MODEL FORMULATION

Let there are k business portals and at an instance t N customers are ready to use for their transactions as shown in following Figure 2. x1, x2, ..., xk are the corresponding fractions which opts business

*Figure 1. Intentionally diversion of original traffic by flooding towards the alternate site*
Related Content

Ripple Effect in Web Applications
[www.igi-global.com/article/ripple-effect-web-applications/44919?camid=4v1a](www.igi-global.com/article/ripple-effect-web-applications/44919?camid=4v1a)

Estimating the Privacy Protection Capability of a Web Service Provider
[www.igi-global.com/chapter/estimating-privacy-protection-capability-web/37723?camid=4v1a](www.igi-global.com/chapter/estimating-privacy-protection-capability-web/37723?camid=4v1a)

SPACots: A Software Tool for Selecting COTS Components
[www.igi-global.com/article/spacots-software-tool-selecting-cots/47028?camid=4v1a](www.igi-global.com/article/spacots-software-tool-selecting-cots/47028?camid=4v1a)

Automating the Generation of Joins in Large Databases and Web Services
[www.igi-global.com/chapter/automating-generation-joins-large-databases/53057?camid=4v1a](www.igi-global.com/chapter/automating-generation-joins-large-databases/53057?camid=4v1a)